Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-03-20 12:47:51
Submitter	Manual Submission
Type	MS OLE document

Analysis Overview

Overall risk level	High risk	The object exhibited highly suspicious characteristics that are commonly associated with malware.	
Detections	TROJ_FRS.0NA103C821		
Exploited vulnerabilities	-		
Analyzed objects	MS OLE document	1 - SWIFT Ref; F607163435808987.xlsx	6CB11FB55788DBCA0262F62475DA412818CCB5DF
	Office Excel 2007 spreadsheet	1.1 - NONAMEFL	47BB2BE32C6C6B8A6AFD5FF22FF1380C054662A4
	Office Word 2007 document	1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm	42F1769E5A244C528AA0660E496FBA7D8B017FCC

Analysis Environments

	Win2012_Office
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	✓

Win2012_Office

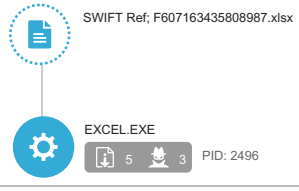
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.0NA103C821
Exploited vulnerabilities	-
Network connection	No network

Object 1 - SWIFT Ref; F607163435808987.xlsx (MS OLE document)

File name	SWIFT Ref; F607163435808987.xlsx
File type	MS OLE document
SHA-1	6CB11FB55788DBCA0262F62475DA412818CCB5DF
SHA-256	1F75301B260414396ABB7790F63B47E5CCDC216CBA57D9B2195CBDA926230EFD
MD5	C797F001BD156DD1B518CC48EA4283FC
Size	2814464 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.0NA103C821
Exploited vulnerabilities	-
Threat Characteristics	File drop, download, sharing, or replication (5) Hijack, redirection, or data theft (3) Malformed, defective, or with known malware traits (1) Suspicious network or messaging activity (18)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Windows Management Instrumentation	Characteristics: 1, 2
Defense Evasion	File Deletion	Characteristics: 1, 2, 3, 4, 5
Discovery	System Information Discovery	Characteristics: 1, 2
	Network Share Discovery	Characteristics: 1

Notable Threat Characteristics

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

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2496 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\FD28D1EE.jpeg Type: VSDT_JPG
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2496 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9EF57D17.jpeg Type: VSDT_JPG
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2496 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\87744B9B.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2496 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\992A98E0.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 2496 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\ADF30361.png Type: VSDT_PNG

Hijack, redirection, or data theft (3)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	■□□	Process ID: 2496 Info: Enums share folder from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2496 Info: Obtains Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%' from API result
Executes commands or uses API to obtain system information	■□□	Process ID: 2496 Info: Obtains Win32_ComputerSystemProduct from API result

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

Characteristic	Significance	Details
Detected as known malware	■■■	Source: ATSE Detection Name: TROJ_FRS.0NA103C821 Engine Version: 12.500.1008 Malware Pattern Version: 16.605.92

Suspicious network or messaging activity (18)

Characteristic	Significance	Details
Listens on port	■□□	0.0.0.0:49182
Listens on port	■□□	0.0.0.0:49181
Listens on port	■□□	0.0.0.0:49180
Listens on port	■□□	0.0.0.0:49179
Listens on port	■□□	0.0.0.0:49178
Listens on port	■□□	0.0.0.0:49177
Listens on port	■□□	0.0.0.0:49176
Listens on port	■□□	0.0.0.0:49175
Listens on port	■□□	0.0.0.0:49174
Listens on port	■□□	127.0.0.1:61707
Listens on port	■□□	0.0.0.0:49173
Listens on port	■□□	0.0.0.0:49172
Listens on port	■□□	0.0.0.0:49171
Listens on port	■□□	0.0.0.0:49170
Listens on port	■□□	0.0.0.0:49169
Listens on port	■□□	0.0.0.0:49168
Listens on port	■□□	0.0.0.0:49167
Listens on port	■□□	0.0.0.0:49166

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
gmail.com	-	53	-	No risk	-	SWIFT Ref; F607163435808987.xlsx
clients2.google.com	-	53	-	No risk	-	SWIFT Ref; F607163435808987.xlsx
self.events.data.microsoft.com	-	53	-	No risk	-	SWIFT Ref; F607163435808987.xlsx
ctldl.windowsupdate.com	-	53	-	No risk	-	SWIFT Ref; F607163435808987.xlsx
www.msftncsi.com	-	53	-	No risk	-	SWIFT Ref; F607163435808987.xlsx
cdn.uci.officeapps.live.com	-	53	-	No risk	-	SWIFT Ref; F607163435808987.xlsx
autodiscover.gmail.com	-	53	-	No risk	-	SWIFT Ref; F607163435808987.xlsx
autodiscover.gmail.com	-	443	-	No risk	-	SWIFT Ref; F607163435808987.xlsx
gmail.com	-	443	-	No risk	-	SWIFT Ref; F607163435808987.xlsx

URL	Site Category	Risk Level	Threat	Accessed By
https://self.events.data.microsoft.com/OneCollector/1.0/	Business / Economy Computers / Internet Cloud Applications	No risk	-	SWIFT Ref; F607163435808987.xlsx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~$SWIFT Ref; F60716343580898 7.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
excel.exe.db-wal	No risk	-	-	-	37112	CE642FD08A7D9CEB93D9542394798ECEFF 55A428
UPTC2SSIN2W8PEDACSFF.tem p	No risk	-	-	-	7682	A3F92AFF41A06C793BF244ED8665F3C6C0 652821
excel.exe.db-shm	No risk	-	-	-	32768	D55EB5837535614767EED7D05842E8B557C 2B9A5
~DFFFF033FA2B5A61E5.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD 7ED4AE5
b8ab77100df80ab2.customDestin ations-ms	No risk	-	-	-	7682	A3F92AFF41A06C793BF244ED8665F3C6C0 652821
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	302	84DE8C3C847B582139A3C85E613CFD460B D97E84
ADF30361.png	No risk	-	-	-	111378	BC754ECEF3BEC86C6AFCC1AF644190AAF C34D9B7
App_1616238045263249000_8A8 200A8-5644-4567-8B5B-A619A9 3A89D4.log	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
App_1616238045260350400_8A8 200A8-5644-4567-8B5B-A619A9 3A89D4.log	No risk	-	-	-	16724	17192BEDBE4298292515DAAE5997347C0C 78E7FE

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	6CB11FB55788DBCA0262F62475DA412818CCB5DF	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.0NA103C821 Engine Version: 12.500.1008 Malware Pattern Version: 16.605.92		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ClientTelemetry\Sampling\1 Value: None		2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2496\ Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2496\0 Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\oi& Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ImmersiveWorkbookDirtySentinel Value: 0		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ExcelWorkbookOpenedCount Value: 0		2496
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\Diagnostics\EXCEL\App_160098525097940 6400_37DFED58-65EC-4733-9903-AF526D736AF9.log) Return: 1		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\EXCEL\2704\0 Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\EXCEL\2704\ Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2496\0 Value: None		2496
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, edabf290) Return: 0		2496
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, edabf290) Return: 0		2496
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, edabf1d0) Return: 0		2496
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2496 Info: Obtains Win32_ComputerSystemProduct from API result		
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0		2496
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, edabf1d0) Return: 0		2496
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2496 Info: Obtains Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%' from API result		
Call WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0		2496
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, edabf1d0) Return: 0		2496
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\f\52C64B7E\LanguageList Value: en-US\0en\0		2496
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, ef64e2b0) Return: 0		2496
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, ef64e2b0) Return: 0		2496
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, ef64e1f0) Return: 0		2496
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0		2496
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, ef64e1f0) Return: 0		2496
Call WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0		2496
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, ef64e1f0) Return: 0		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastSyncTimeExcel Value: None		2496

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastWriteTimeExcel Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\oi& Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\'w& Value: None		2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CBB88\ Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CBB88\1CBB88 Value: None		2496
Call System API	API Name: CryptDeriveKey Args: (eeb93d20, 660e, f1f13d90, 800000, e3a289e0) Return: 1		2496
Call System API	API Name: CryptDeriveKey Args: (eeb93d20, 660e, f1f0f720, 800000, f1ddab28) Return: 1		2496
Call System API	API Name: CryptDeriveKey Args: (eeb93d20, 660e, f1f0ea00, 800000, f1ddab28) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ².9ÿ3Ø¿×ï, 16, 0, , 0, ².9ÿ3Ø¿×ï, 16, -475886256, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, e3a28d88, 10) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, S\r?», 32, 0, , 0, S\r?», 32, -475886256, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1e966b0, 20) Return: 1		2496
Call System API	API Name: CryptDeriveKey Args: (eeb96720, 660e, f1f0e990, 800000, f1ddd508) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, PK, 4096, 0, , 0, PK, 4096, -475885232, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 3296, 0, , 0, , 3296, -475887008, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, ce0) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, PK, 4096, 0, , 0, PK, 4096, -475889568, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ExcelWorkbookOpenedCount Value: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ¾¦¥ºÏ, 4096, 0, , 0, ¾¦¥ºÏ, 4096, -475896800, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ú`¦X QPF•, 4096, 0, , 0, ú`¦X QPF•, 4096, -475896800, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ?à , 4096, 0, , 0, ?à , 4096, -475896800, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, „)x, 4096, 0, , 0, „)x, 4096, -475896800, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ì~ÝÜ[ï¼¯Öku5²™ Ü\rÃ, 4096, 0, , 0, ì~ÝÜ[ï¼¯Öku5²™ Ü\rÃ, 4096, -475896800, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, PÐ, 4096, 0, , 0, PÐ, 4096, -475896800, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, øõ1~ûq, 4096, 0, , 0, øõ1~ûq, 4096, -475896800, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475896832, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, %-V]·:, 4096, 0, , 0, %-V]·:, 4096, -475896800, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ïnN, 4096, 0, , 0, ïnN, 4096, -475896800, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, 'Úì, 4096, 0, , 0, 'Úì, 4096, -475896800, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 3296, 0, , 0, , 3296, -475897872, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, ce0) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, PK, 4096, 0, , 0, PK, 4096, -475896496, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CBB88\1CBB88 Value: None		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475896576, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, %-V]·:, 4096, 0, , 0, %-V]·:, 4096, -475898336, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, „)x, 4096, 0, , 0, „)x, 4096, -475902368, 0) Return: 0		2496
Call System API	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, 'Úì, 4096, 0, , 0, 'Úì, 4096, -475900880, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475897968, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, –qŒg, 4096, 0, , 0, –qŒg, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ä´¶ xªQÄ"ñÏÎÍQ'ì, 4096, 0, , 0, ä´¶ xªQÄ"ñÏÎÍQ'ì, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, É;tœÒÐg ×¶ƒÃc-™?³,Pà‡æƒÐ, 4096, 0, , 0, É;tœÒÐg ×¶ƒÃc-™?³,Pà‡æƒÐ, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ÏCü²ëäe†¡Ù'€Îž "Z„tã2, 4096, 0, , 0, ÏCü²ëäe†¡Ù'€Îž "Z„tã2, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, \r‹†ú, 4096, 0, , 0, \r‹†ú, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, `8öñ‹ÆôV©³¢§'š, 4096, 0, , 0, `8öñ‹ÆôV©³¢§'š, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, 5Ú, 4096, 0, , 0, 5Ú, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ÉÁÇ1Y^, 4096, 0, , 0, ÉÁÇ1Y^, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, 2{D£ÕuÔ†'\rlf„9"5¿"ŒÜÁP[k|H±, 4096, 0, , 0, 2{D£ÕuÔ†'\rlf„9"5¿"ŒÜÁP[k|H±, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, [P+/"E„Žžodî, 4096, 0, , 0, [P+/"E„Žžodî, 4096, -475902688, 0) Return: 0		2496

Call System API	API Name: BCryptDecrypt Args: (f1ec6430, FÕÓÖ½}_“, 4096, 0, , 0, FÕÓÖ½}_“, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, IsF5, 4096, 0, , 0, IsF5, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, q'_Úfªø'¢ZÈÀV, 4096, 0, , 0, q'_Úfªø'¢ZÈÀV, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, gš®, 4096, 0, , 0, gš®, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, D¶, 4096, 0, , 0, D¶, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, £¨¦Ÿ, 4096, 0, , 0, £¨¦Ÿ, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ™ÒŠ7, 4096, 0, , 0, ™ÒŠ7, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, €, 0\rXG, 4096, 0, , 0, €, 0\rXG, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, à, 4096, 0, , 0, à, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Ý«Ñ^Aá†¾69¥, Aikt†, 4096, 0, , 0, Ý«Ñ^Aá†¾69¥, Aikt†, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, (, 4096, 0, , 0, (, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, æÍ}‡ZÊ‚š®äî¿&}=fpÅ82™, 4096, 0, , 0, æÍ}‡ZÊ‚š®äî¿&}=fpÅ82™, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, %!ÊóÙ|7T\Å¤, 4096, 0, , 0, %!ÊóÙ|7T\Å¤, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ëÅJ$ á0\nÞ-‚š, 4096, 0, , 0, ëÅJ$ á0\nÞ-‚š, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ØñEÔ Ä·Ž»cž, 4096, 0, , 0, ØñEÔ Ä·Ž»cž, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, _DgB`°, 4096, 0, , 0, _DgB`°, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ÃA"ñ·wwÁwuTbÔ|, 4096, 0, , 0, ÃA"ñ·wwÁwuTbÔ|, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, *mÿ(, 4096, 0, , 0, *mÿ(, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ™×¬£é, 4096, 0, , 0, ™×¬£é, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ôÈV—S\†K, 4096, 0, , 0, ôÈV—S\†K, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, õ?Ñ]WsyaÂBû»/€Ài0ÎHÀ„Æº^h´p, 4096, 0, , 0, õ?Ñ]WsyaÂBû»/€Ài0ÎHÀ„Æº^h´p, 4096, -475902688, 0) Return : 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, î'¥"ØÇÑ×~Þ¯hèlv½Un, 4096, 0, , 0, î'¥"ØÇÑ×~Þ¯hèlv½Un, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ¬þWa÷"äÔ, 4096, 0, , 0, ¬þWa÷"äÔ, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ÔÞ\rüQn2ÈbRÎ, 4096, 0, , 0, ÔÞ\rüQn2ÈbRÎ, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, (", 4096, 0, , 0, (", 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Yg, 4096, 0, , 0, Yg, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, –wÎ°Ë°"Nÿ‰ê¤, 4096, 0, , 0, –wÎ°Ë°"Nÿ‰ê¤, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ÷il}èg, 4096, 0, , 0, ÷il}èg, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ;mÓ¸æK¢ÝÊ, 4096, 0, , 0, ;mÓ¸æK¢ÝÊ, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ´:ù, 4096, 0, , 0, ´:ù, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, =Ž‡›C¬óÑ‹rÎÝ½ò¸ÏÜrÄbç \nÒõw#þÊ:i", 4096, 0, , 0, =Ž‡›C¬óÑ‹rÎÝ½ò¸ÏÜrÄbç \nÒõw#þÊ:i", 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Ž«, 4096, 0, , 0, Ž«, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ¼, a 3ªâÜ1Õ-H_0D%)k, %²7[, 4096, 0, , 0, ¼, a 3ªâÜ1Õ-H_0D%)k, %²7[, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, :é8Ózìßàu, 4096, 0, , 0, :é8Ózìßàu, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, dÖÍ¯1¢ÊƒµèI, 4096, 0, , 0, dÖÍ¯1¢ÊƒµèI, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ¶×;2©3ÿXû]¯84¯¯ló¾v, 4096, 0, , 0, ¶×;2©3ÿXû]¯84¯¯ló¾v, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ª, 4096, 0, , 0, ª, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Ûïy¨òg73Ó91^Û õt{ñRC¼Ôè*èzJ, 4096, 0, , 0, Ûïy¨òg73Ó91^Û õt{ñRC¼Ôè*èzJ, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ÕÙ{÷I, 4096, 0, , 0, ÕÙ{÷I, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ë), 4096, 0, , 0, ë), 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, èl'xÍØ]l@), 4096, 0, , 0, èl'xÍØ]l@), 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ²[æ³{û±(•bï€ÕOj, 4096, 0, , 0, ²[æ³{û±(•bï€ÕOj, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, §g' u¡}u±/õ, 4096, 0, , 0, §g' u¡}u±/õ, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ëË¿, 4096, 0, , 0, ëË¿, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, '[§kß, 4096, 0, , 0, '[§kß, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Ê, 4096, 0, , 0, Ê, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, éBÇ¿Á, 4096, 0, , 0, éBÇ¿Á, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ^K¯øü/—?•€, 4096, 0, , 0, ^K¯øü/—?•€, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Ú, 4096, 0, , 0, Ú, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ‖µ¯ŸxÖÞ0ºÉ^"ðY, 4096, 0, , 0, ‖µ¯ŸxÖÞ0ºÉ^"ðY, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, š'ö¯\¿Þ|ÄUxDÔ—Ô"S¤7—òI,LùëÐ»½ð@, 4096, 0, , 0, š'ö¯\¿Þ|ÄUxDÔ—Ô"S¤7—òI,LùëÐ»½ð@, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, q¸ú, 4096, 0, , 0, q¸ú, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, (2•Í, 4096, 0, , 0, (2•Í, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Ì÷Ñ, 4096, 0, , 0, Ì÷Ñ, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, j, 4096, 0, , 0, j, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, 3ùQ„¼Ž"¿, 4096, 0, , 0, 3ùQ„¼Ž"¿, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, à, 4096, 0, , 0, à, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, …Øü³, 4096, 0, , 0, …Øü³, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ¢¯, 4096, 0, , 0, ¢¯, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ÐfŒ*, 4096, 0, , 0, ÐfŒ*, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ä¤×½, 4096, 0, , 0, ä¤×½, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, O>`ú, , 4096, 0, , 0, O>`ú, , 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, \nd¯±eÕ€, 4096, 0, , 0, \nd¯±eÕ€, 4096, -475902688, 0) Return: 0		2496

Call System API	API Name: BCryptDecrypt Args: (f1ec6430, 2, 4096, 0, , 0, 2, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ß ^Ái¼m, 4096, 0, , 0, ß ^Ái¼m, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, $,+, 4096, 0, , 0, $,+, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Æ, 4096, 0, , 0, Æ, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Òº, 4096, 0, , 0, Òº, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ½®»Ò¦fk, 4096, 0, , 0, ½®»Ò¦fk, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, 8ùùôã»¦×0ý\Âq, 4096, 0, , 0, 8ùùôã»¦×0ý\Âq, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ´H'íÎ£G²Ô, 4096, 0, , 0, ´H'íÎ£G²Ô, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Ý, ••WZÙ#Đu$êXþ"Ôf¾t´¥õ™a¦/níW¤3?D}ÍÓ‡‹'", 4096, 0, , 0, Ý, ••WZÙ#Đu$êXþ"Ôf¾t´¥õ™a¦/níW¤3?D}ÍÓ‡‹'", 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Y£; ^, 4096, 0, , 0, Y£; ^, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ¤ayü\l}ú¯Ü, 4096, 0, , 0, ¤ayü\l}ú¯Ü, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ,, 4096, 0, , 0, ,, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, "\r~, 4096, 0, , 0, "\r~, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Õi$AöæÄâty ñ+¼õGžæºÏ3, 4096, 0, , 0, Õi$AöæÄâty ñ+¼õGžæºÏ3, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, RÝ, 4096, 0, , 0, RÝ, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, è, 4096, 0, , 0, è, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ¥¢9, 4096, 0, , 0, ¥¢9, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, žóêÂ¢´1., 4096, 0, , 0, žóêÂ¢´1., 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, érM, 4096, 0, , 0, érM, 4096, -475902688, 0) Return: 0		2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Ù¨æ—Ûõõu, 4096, 0, , 0, Ù¨æ—Ûõõu, 4096, -475902688, 0) Return: 0		2496
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (ef84e4f0, 0, 0, 0) Return: 1		2496
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0004		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2496
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (ef84e390, 0, 0, 0) Return: 1		2496
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (ef84e360, 0, 0, 0) Return: 1		2496
Call Network API	API Name: socket Args: (23, 1, 6) Return: 94c		2496
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		2496
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2496) Return: 1		2496
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\Program) Return: 1		2496
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2496) Return: 1		2496
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2496
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -235334240) Return: cc0008		2496
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -201853368, -2067004672, -235334240) Return: cc000c		2496
Call System API	API Name: WinHttpCloseHandle Args: (f1efad00) Return: 1		2496
Call Network API	API Name: socket Args: (2, 2, 0) Return: b1c		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: b1c		2496
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87		2496
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: b28		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: b28		2496
Call Network API	API Name: bind Args: (b28, 0.0.0.0:49166, 16) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49166		
Call System API	API Name: ConnectEx Args: (b28, self.events.data.microsoft.com:443, 16, 0, 0, 0, eea7c8d8) Return: 0		2496
Call Network API	API Name: send Args: (b28, ..., 1, 191) Return: 0		2496
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2496
Call System API	API Name: WinHttpCloseHandle Args: (f1efb450) Return: 1		2496
Call Network API	API Name: socket Args: (23, 1, 6) Return: d98		2496
Call Network API	API Name: socket Args: (2, 2, 0) Return: df4		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: df4		2496
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2496
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: d88		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: d88		2496
Call Network API	API Name: bind Args: (d88, 0.0.0.0:49167, 128) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49167		
Call System API	API Name: ConnectEx Args: (d88, ctldl.windowsupdate.com:80, 16, 0, 0, 0, f1f3b958) Return: 0		2496
Call Network API	API Name: send Args: (d88, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?64ddc54b9581b1b6 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0		2496
Call System API	API Name: WinHttpCloseHandle Args: (f22ee250) Return: 1		2496

Call System API	API Name: WinHttpCloseHandle Args: (f1f396e0) Return: 1		2496
Call System API	API Name: WinHttpCloseHandle Args: (eec2c6e0) Return: 1		2496
Call Network API	API Name: socket Args: (23, 1, 6) Return: d80		2496
Call System API	API Name: WinHttpCloseHandle Args: (f1efb6c0) Return: 1		2496
Call Network API	API Name: socket Args: (2, 2, 0) Return: e24		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: e24		2496
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2496
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: df4		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: df4		2496
Call Network API	API Name: bind Args: (df4, 0.0.0.0:49168, 128) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49168		
Call System API	API Name: ConnectEx Args: (df4, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, f1f3b3d8) Return: 0		2496
Call Network API	API Name: send Args: (df4, ..., 1, 188) Return: 0		2496
Call System API	API Name: WinHttpCloseHandle Args: (f22edb30) Return: 1		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: df4		2496
Call Network API	API Name: bind Args: (df4, 0.0.0.0:49169, 128) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49169		
Call System API	API Name: ConnectEx Args: (df4, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, f1f3c198) Return: 0		2496
Call Network API	API Name: send Args: (df4, ..., 1, 188) Return: 0		2496
Call System API	API Name: WinHttpCloseHandle Args: (f22efb40) Return: 1		2496
Call System API	API Name: WinHttpCloseHandle Args: (f1f3afa0) Return: 1		2496
Call System API	API Name: WinHttpCloseHandle Args: (f1f3b100) Return: 1		2496
Call System API	API Name: WinHttpCloseHandle Args: (f1efad00) Return: 1		2496
Call Network API	API Name: socket Args: (2, 2, 0) Return: e38		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: e38		2496
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2496
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: e24		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: e24		2496
Call Network API	API Name: bind Args: (e24, 0.0.0.0:49170, 128) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49170		
Call System API	API Name: ConnectEx Args: (e24, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, f1f3c198) Return: 0		2496
Call Network API	API Name: send Args: (e24, ..., 1, 188) Return: 0		2496
Call System API	API Name: WinHttpCloseHandle Args: (f22efb40) Return: 1		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: e24		2496
Call Network API	API Name: bind Args: (e24, 0.0.0.0:49171, 128) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49171		
Call System API	API Name: ConnectEx Args: (e24, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, f1f3b538) Return: 0		2496
Call Network API	API Name: send Args: (e24, ..., 1, 188) Return: 0		2496
Call System API	API Name: WinHttpCloseHandle Args: (f22efb40) Return: 1		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: e24		2496
Call Network API	API Name: bind Args: (e24, 0.0.0.0:49172, 128) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49172		
Call System API	API Name: ConnectEx Args: (e24, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, f1f3b958) Return: 0		2496
Call Network API	API Name: send Args: (e24, ..., 1, 188) Return: 0		2496
Call System API	API Name: WinHttpCloseHandle Args: (f22efb40) Return: 1		2496
Call System API	API Name: WinHttpCloseHandle Args: (f1f396e0) Return: 1		2496
Call System API	API Name: WinHttpCloseHandle Args: (f1f3b100) Return: 1		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: e24		2496
Call Network API	API Name: bind Args: (e24, 0.0.0.0:49173, 128) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49173		
Call System API	API Name: ConnectEx Args: (e24, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, f1f3b538) Return: 0		2496
Call Network API	API Name: send Args: (e24, ..., 1, 188) Return: 0		2496
Call System API	API Name: WinHttpCloseHandle Args: (f22edb30) Return: 1		2496
Call System API	API Name: WinHttpCloseHandle Args: (f1f38d40) Return: 1		2496
Call Network API	API Name: socket Args: (2, 2, 0) Return: 298		2496
Call Network API	API Name: bind Args: (298, 127.0.0.1:61707, 128) Return: 0		2496
Detection	Threat Characteristic: Listens on port 127.0.0.1:61707		
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII		2496
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CBB88\1CBB88 Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CBB88\ Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\'w& Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2496

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CEC6C\ Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CEC6C\1CEC6C Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2496\0 Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2496\0 Value: None		2496
Call Network API	API Name: socket Args: (2, 1, 0) Return: 1014		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\SessionId Value: None		2496
Call System API	API Name: WinHttpCloseHandle Args: (f6e42920) Return: 1		2496
Call Network API	API Name: socket Args: (2, 2, 0) Return: 103c		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: 103c		2496
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87		2496
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: 103c		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: 103c		2496
Call Network API	API Name: bind Args: (103c, 0.0.0.0:49174, 128) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49174		
Call System API	API Name: ConnectEx Args: (103c, gmail.com:443, 16, 0, 0, 0, f6ea7118) Return: 0		2496
Call Network API	API Name: send Args: (103c, ..., 1, 170) Return: 0		2496
Call System API	API Name: WinHttpCloseHandle Args: (f70dade0) Return: 1		2496
Call System API	API Name: WinHttpCloseHandle Args: (f6ea5840) Return: 1		2496
Call Network API	API Name: socket Args: (2, 2, 0) Return: 1040		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: 1040		2496
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1, 40006000) Return: 87		2496
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1c, 40026000) Return: 9003		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: 1040		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1040		2496
Call Network API	API Name: bind Args: (1040, 0.0.0.0:49175, 128) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49175		
Call System API	API Name: ConnectEx Args: (1040, autodiscover.gmail.com:443, 16, 0, 0, 0, f6ea6098) Return: 0		2496
Call Network API	API Name: send Args: (1040, ..., 1, 183) Return: 0		2496
Call System API	API Name: WinHttpCloseHandle Args: (f70dcdf0) Return: 1		2496
Call System API	API Name: WinHttpCloseHandle Args: (f6ea8440) Return: 1		2496
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2496
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -232109136) Return: cc0008		2496
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -201853368, -2067004672, -232109136) Return: cc000c		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: 102c		2496
Call Network API	API Name: bind Args: (102c, 0.0.0.0:49176, 16) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49176		
Call System API	API Name: ConnectEx Args: (102c, self.events.data.microsoft.com:443, 16, 0, 0, 0, f6e93b48) Return: 0		2496
Call Network API	API Name: send Args: (102c, ..., 1, 191) Return: 0		2496
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2496
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -2118239504) Return: cc0008		2496
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -201853368, -2067004672, -2118239504) Return: cc000c		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: 68c		2496
Call Network API	API Name: bind Args: (68c, 0.0.0.0:49177, 16) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call System API	API Name: ConnectEx Args: (68c, self.events.data.microsoft.com:443, 16, 0, 0, 0, f6e96708) Return: 0		2496
Call Network API	API Name: send Args: (68c, ..., 1, 191) Return: 0		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\File MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\File MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\		2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\User MRU\LiveId_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C495056D56BADD0D4\File MRU\ Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\User MRU\LiveId_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C495056D56BADD0D4\File MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\User MRU\LiveId_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C495056D56BADD0D4\File MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\		2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Place MRU\ Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Place MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Place MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\		2496
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2496
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -150654704) Return: cc0008		2496
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -201853368, -2067004672, -150654704) Return: cc000c		2496
Call System API	API Name: WinHttpCloseHandle Args: (f6e448d0) Return: 1		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1034		2496
Call Network API	API Name: bind Args: (1034, 0.0.0.0:49178, 16) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49178		
Call System API	API Name: ConnectEx Args: (1034, self.events.data.microsoft.com:443, 16, 0, 0, 0, f6e907a8) Return: 0		2496
Call Network API	API Name: send Args: (1034, ..., 1, 191) Return: 0		2496

Call System API	API Name: WinHttpCloseHandle Args: (f6e437c0) Return: 1		2496
Call Network API	API Name: socket Args: (2, 2, 0) Return: 1060		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: 1060		2496
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2496
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: e38		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: e38		2496
Call Network API	API Name: bind Args: (e38, 0.0.0.0:49179, 128) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49179		
Call System API	API Name: ConnectEx Args: (e38, ctldl.windowsupdate.com:80, 16, 0, 0, 0, f6ae5498) Return: 0		2496
Call Network API	API Name: send Args: (e38, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f8d25b66fe4dab7a HTTP/1.1\r\nConnection: Keep-Alive\r\n Accept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0		2496
Call System API	API Name: WinHttpCloseHandle Args: (f6e355e0) Return: 1		2496
Call System API	API Name: WinHttpCloseHandle Args: (f6ae5f80) Return: 1		2496
Call System API	API Name: WinHttpCloseHandle Args: (f7050820) Return: 1		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xls\OpenWithProgids\Excel.Sheet.8 Value: None		2496
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 1fcc1318, -1, ef54d270, ef54d278, 0) Return: 0		2496
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2496 Info: Enums share folder from API result		
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\UPTC2SSIN2W8PEDACSFF.temp Type: VSDT_COM_DOS		2496
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\UPTC2SSIN2W8PEDACSFF.temp Type: VSDT_COM_DOS		2496
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\b8ab77100df80ab2.customDestinations-ms Type: VSDT_COM_DOS		2496
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{9B92EB61-CBC1-11D3-8C2D-00A0CC37B591}\1.2\(Default) Value: Microsoft Smart Tags 2.0 Type Library		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-A27D-11D3-BD33-D80C46980A07}\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-A27D-11D3-BD33-D80C46980A07}\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-A27D-11D3-BD33-D80C46980A07}\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-A27D-11D3-BD33-D80C46980A07}\ProxyStubClsid32\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-A27D-11D3-BD33-D80C46980A07}\ProxyStubClsid32\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-A27D-11D3-BD33-D80C46980A07}\ProxyStubClsid32\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-A27D-11D3-BD33-D80C46980A07}\TypeLib\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-A27D-11D3-BD33-D80C46980A07}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-A27D-11D3-BD33-D80C46980A07}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-A27D-11D3-BD33-D80C46980A07}\TypeLib\Version Value: 1.2		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\ProxyStubClsid32\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\ProxyStubClsid32\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\ProxyStubClsid32\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\TypeLib\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\TypeLib\Version Value: 1.2		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\ProxyStubClsid32\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\ProxyStubClsid32\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\ProxyStubClsid32\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\TypeLib\ Value: None		2496

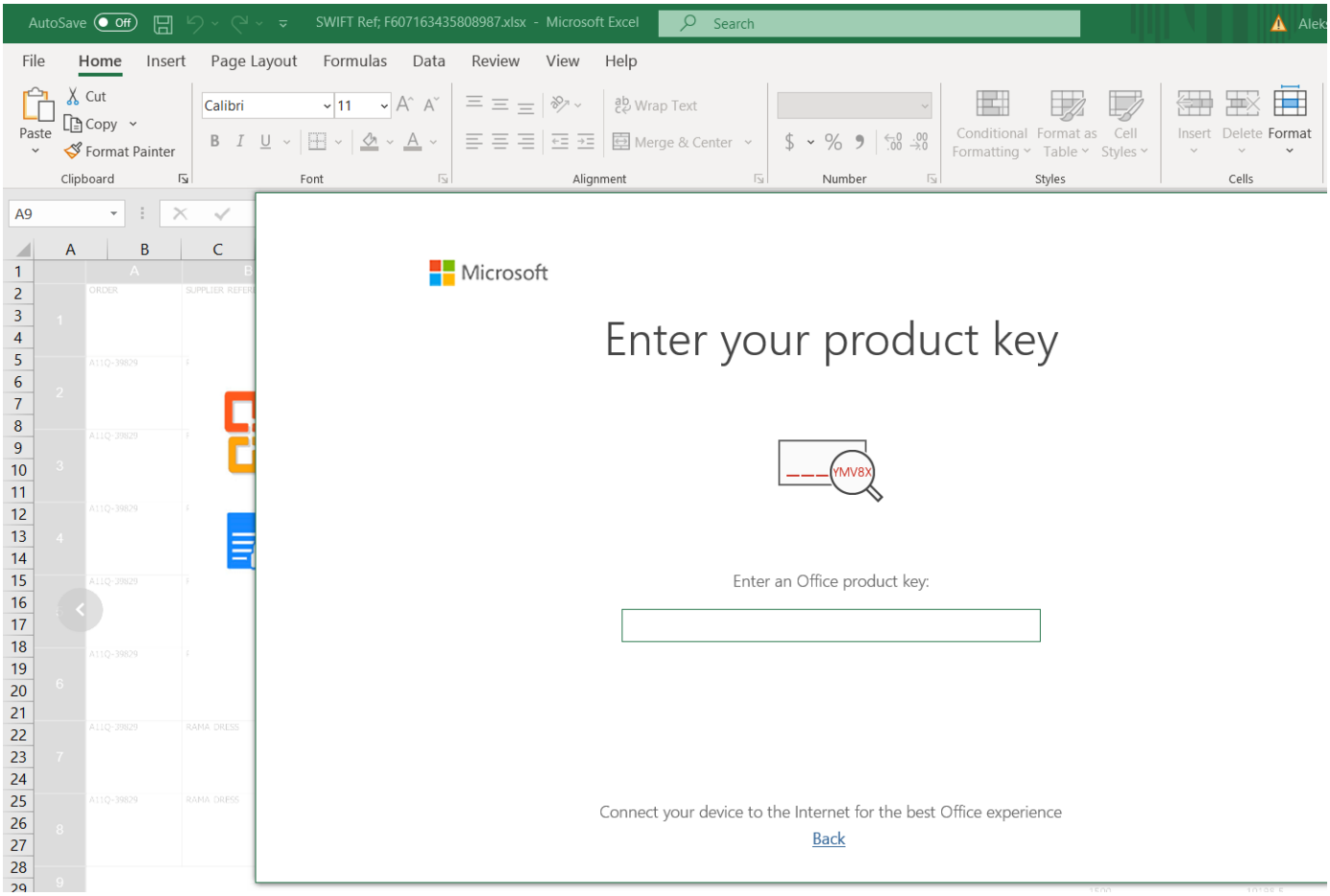
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\TypeLib\Version Value: 1.2		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\ProxyStubClsid32\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\ProxyStubClsid32\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\ProxyStubClsid32\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\TypeLib\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\TypeLib\Version Value: 1.2		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\ProxyStubClsid32\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\ProxyStubClsid32\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\ProxyStubClsid32\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\TypeLib\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\TypeLib\Version Value: 1.2		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{347958C0-E86F-4865-97C8-BED31E4C28E0}\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{347958C0-E86F-4865-97C8-BED31E4C28E0}\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{347958C0-E86F-4865-97C8-BED31E4C28E0}\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{347958C0-E86F-4865-97C8-BED31E4C28E0}\ProxyStubClsid32\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{347958C0-E86F-4865-97C8-BED31E4C28E0}\ProxyStubClsid32\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{347958C0-E86F-4865-97C8-BED31E4C28E0}\ProxyStubClsid32\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{347958C0-E86F-4865-97C8-BED31E4C28E0}\TypeLib\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{347958C0-E86F-4865-97C8-BED31E4C28E0}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{347958C0-E86F-4865-97C8-BED31E4C28E0}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{347958C0-E86F-4865-97C8-BED31E4C28E0}\TypeLib\Version Value: 1.2		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A4}\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A4}\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A4}\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A4}\ProxyStubClsid32\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A4}\ProxyStubClsid32\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A4}\ProxyStubClsid32\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A4}\TypeLib\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A4}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A4}\TypeLib\(Default) Value: None		2496

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A4}\TypeLib\Version Value: 1.2		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\ProxyStubClsid32\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\ProxyStubClsid32\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\ProxyStubClsid32\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\TypeLib\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\TypeLib\Version Value: 1.2		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\ProxyStubClsid32\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\ProxyStubClsid32\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\ProxyStubClsid32\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\TypeLib\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\TypeLib\Version Value: 1.2		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\(Default) Value: None		2496
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\ProxyStubClsid32\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\ProxyStubClsid32\(Default) Value: None		2496
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -289128768) Return: cc0008		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\ProxyStubClsid32\(Default) Value: None		2496
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -201853368, -2067004672, -289128768) Return: cc000c		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\TypeLib\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\TypeLib\Version Value: 1.2		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\ProxyStubClsid32\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\ProxyStubClsid32\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\ProxyStubClsid32\(Default) Value: None		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: 9b8		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\TypeLib\ Value: None		2496
Call Network API	API Name: bind Args: (9b8, 0.0.0.0:49180, 16) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49180		

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\TypeLib\Version Value: 1.2		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\ProxyStubClsid32\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\ProxyStubClsid32\(Default) Value: None		2496
Call System API	API Name: ConnectEx Args: (9b8, self.events.data.microsoft.com:443, 16, 0, 0, 0, f6e99178) Return: 0		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\ProxyStubClsid32\(Default) Value: None		2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\TypeLib\ Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\TypeLib\(Default) Value: None		2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\TypeLib\Version Value: 1.2		2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\ Value: None		2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\ Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\FriendlyName Value: Microsoft Excel		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\LabelText Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\Save Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\ShowButtons Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\ShowIndicators Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\NoLabelOption Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\NoSaveOption Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\NoButtonOption Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\NoIndicatorOption Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CEC6C\1CEC6C Value: None		2496
Call Filesystem API	API Name: RemoveDirectoryW Args: (%TEMP%\{301A5DC2-3F0C-45DF-B987-9AF490E6D994}\ ) Return: 1		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CEC6C\ Value: None		2496
Call Network API	API Name: send Args: (9b8, ..., 1, 191) Return: 0		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ImmersiveWorkbookDirtySentinel Value: 7fffffff		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2496\0 Value: None		2496
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\ADF30361.png Type: VSDT_PNG		2496
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\ADF30361.png Type: VSDT_PNG		2496
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\ADF30361.png Type: VSDT_PNG		2496
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2496 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\ADF30361.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\992A98E0.png Type: VSDT_PNG		2496
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\992A98E0.png Type: VSDT_PNG		2496
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\992A98E0.png Type: VSDT_PNG		2496
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2496 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\992A98E0.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\87744B9B.png Type: VSDT_PNG		2496
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\87744B9B.png Type: VSDT_PNG		2496
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\87744B9B.png Type: VSDT_PNG		2496
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2496 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\87744B9B.png Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9EF57D17.jpeg Type: VSDT_JPG		2496
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9EF57D17.jpeg Type: VSDT_JPG		2496
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9EF57D17.jpeg Type: VSDT_JPG		2496
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2496 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9EF57D17.jpeg Type: VSDT_JPG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\FD28D1EE.jpeg Type: VSDT_JPG		2496
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\FD28D1EE.jpeg Type: VSDT_JPG		2496
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\FD28D1EE.jpeg Type: VSDT_JPG		2496

Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2496 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\FD28D1EE.jpeg Type: VSDT_JPG		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\293B1D82.emf) Return: 1		2496
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2496
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -232108112) Return: cc0010		2496
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0010, POST, /OneCollector/1.0/, , , -201853368, -2067004672, -232108112) Return: cc0014		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: 598		2496
Call Network API	API Name: bind Args: (598, 0.0.0.0:49181, 16) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49181		
Call System API	API Name: ConnectEx Args: (598, self.events.data.microsoft.com:443, 16, 0, 0, 0, f6e94ef8) Return: 0		2496
Call Network API	API Name: send Args: (598, ..., 1, 191) Return: 0		2496
Call System API	API Name: WinHttpCloseHandle Args: (f6e426b0) Return: 1		2496
Call Network API	API Name: socket Args: (2, 2, 0) Return: 6a0		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: 6a0		2496
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2496
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2496
Call Network API	API Name: socket Args: (23, 2, 0) Return: 6a0		2496
Call Network API	API Name: socket Args: (2, 1, 6) Return: 6a0		2496
Call Network API	API Name: bind Args: (6a0, 0.0.0.0:49182, 128) Return: 0		2496
Detection	Threat Characteristic: Listens on port 0.0.0.0:49182		
Call System API	API Name: ConnectEx Args: (6a0, ctldl.windowsupdate.com:80, 16, 0, 0, 0, f6aec818) Return: 0		2496
Call Network API	API Name: send Args: (6a0, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9aa4e523a84d64eb HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0		2496
Call System API	API Name: WinHttpCloseHandle Args: (f732a740) Return: 1		2496
Call System API	API Name: WinHttpCloseHandle Args: (f6aeb200) Return: 1		2496
Call System API	API Name: WinHttpCloseHandle Args: (f22f2ef0) Return: 1		2496

Screenshot



Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	47BB2BE32C6C6B8A6AFD5FF22FF1380C054662A4
SHA-256	49CB1E34DB1EDC4F45178E1F7DA9EEB4B79112F41A16684E100E107842B36042
MD5	97B64B59A5CD7C5E39235444D7C6D103
Size	2788567 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
cdn.uci.officeapps.live.com	-	53	-	No risk	-	NONAMEFL
clients2.google.com	-	53	-	No risk	-	NONAMEFL
ctldl.windowsupdate.com	-	53	-	No risk	-	NONAMEFL
self.events.data.microsoft.com	-	53	-	No risk	-	NONAMEFL
www.msftncsi.com	-	53	-	No risk	-	NONAMEFL
gmail.com	-	53	-	No risk	-	NONAMEFL
autodiscover.gmail.com	-	53	-	No risk	-	NONAMEFL
autodiscover.gmail.com	-	443	-	No risk	-	NONAMEFL
gmail.com	-	443	-	No risk	-	NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
https://self.events.data.microsoft.com/OneCollector/1.0/	Business / Economy Computers / Internet Cloud Applications	No risk	-	NONAMEFL

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
excel.exe.db-shm	No risk	-	-	-	32768	D4F87270D99C1B3CFD83FA16358FDD400F79050F
~$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
excel.exe.db-wal	No risk	-	-	-	4152	FE9AEFBCC9EAA3154B13965A64473821C1DBF459
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	302	64468F3F568586DB742F3908FC13A079196BE298
App_1616237907177800100_18728FC5-2DD3-4F90-BBDB-9CA7C1B51E0A.log	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
8F82FDC5.emf	No risk	-	-	-	653280	333C8CD569694A103E049EC626C173C9AA5673D0
6DDB91B.png	No risk	-	-	-	51166	85B228BBC80DC60D40F4D3473E10B742E7B9039E
{18728FC5-2DD3-4F90-BBDB-9CA7C1B51E0A} - OProcSessId.dat	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
43006102.png	No risk	-	-	-	79394	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
App_1616237907173854200_18728FC5-2DD3-4F90-BBDB-9CA7C1B51E0A.log	No risk	-	-	-	16694	6DCA62FF92E7321ED6B78195602744A7CB74456B

Analysis

Event Type	Details	Parent PID	PID
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ClientTelemetry\Sampling\1 Value: None		2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2404\ Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2404\0 Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\&% Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ImmersiveWorkbookDirtySentinel Value: 0		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ExcelWorkbookOpenedCount Value: 0		2404
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\Diagnostics\EXCEL\App_1600985250979406400_37DFED58-65EC-4733-9903-AF526D736AF9.log) Return: 1		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\EXCEL\2704\0 Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\EXCEL\2704\ Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2404\0 Value: None		2404
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, 6f2ff5d0) Return: 0		2404
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 6f2ff5d0) Return: 0		2404
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 6f2ff510) Return: 0		2404
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0		2404
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, 6f2ff510) Return: 0		2404
Call WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0		2404
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, 6f2ff510) Return: 0		2404
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\f\52C64B7E\LanguageList Value: en-US\0en\0		2404
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, 6f83e0c0) Return: 0		2404
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 6f83e0c0) Return: 0		2404
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 6f83e000) Return: 0		2404
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0		2404
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, 6f83e000) Return: 0		2404

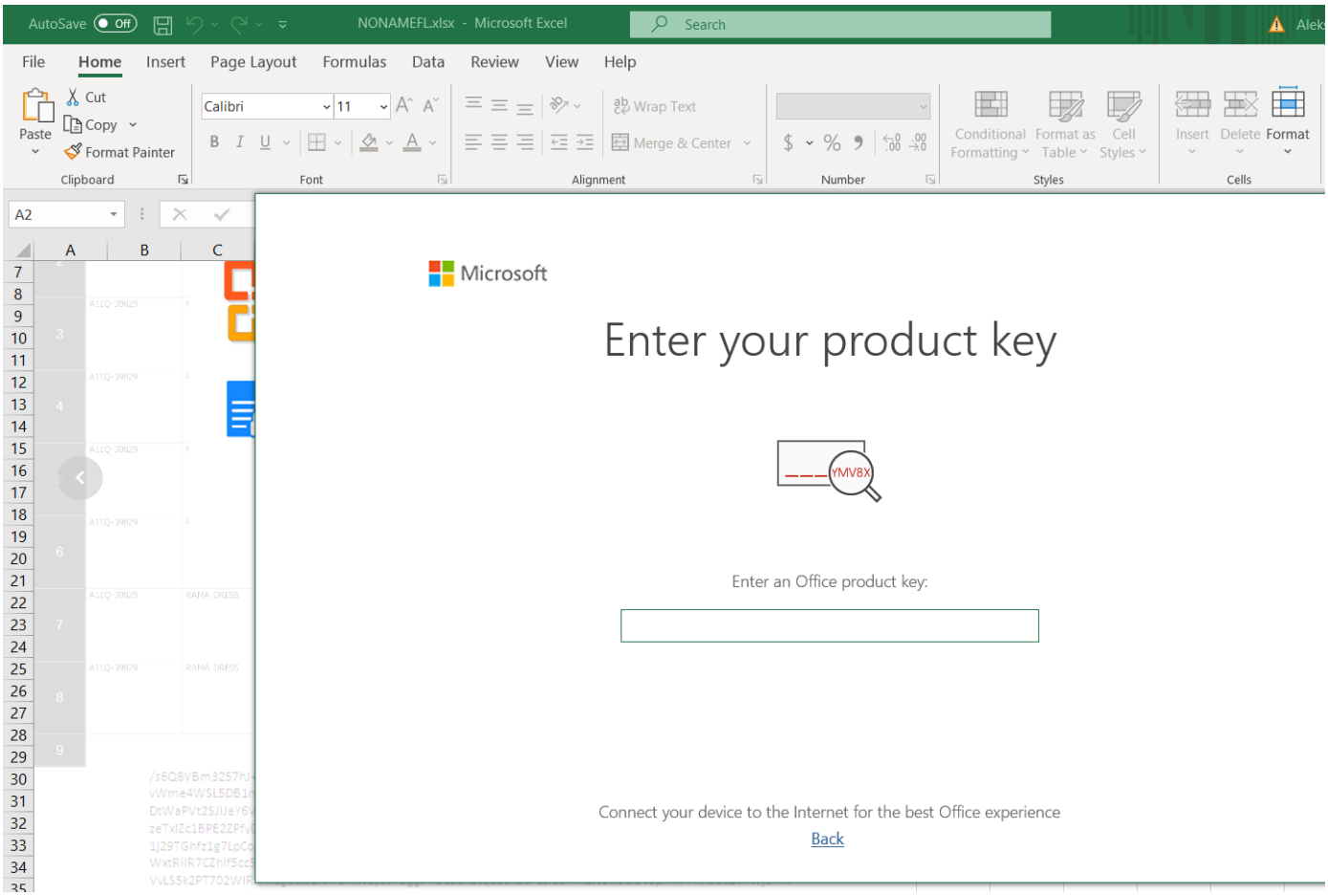
Call WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0		2404
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, 6f83e000) Return: 0		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastSyncTimeExcel Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastWriteTimeExcel Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\&% Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2404\0 Value: None		2404
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (6f2fe470, 0, 0, 0) Return: 1		2404
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0004		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2404
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (6f2fe310, 0, 0, 0) Return: 1		2404
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (6f2fe2e0, 0, 0, 0) Return: 1		2404
Call Network API	API Name: socket Args: (23, 1, 6) Return: a30		2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems|*& Value: None		2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CCA5D\ Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CCA5D\1CCA5D Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ExcelWorkbookOpenedCount Value: 1		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CCA5D\1CCA5D Value: None		2404
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		2404
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2404) Return: 1		2404
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2404
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 1880442320) Return: cc0008		2404
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2022699000, -2067004672, 1880442320) Return: cc000c		2404
Call Network API	API Name: socket Args: (2, 2, 0) Return: c14		2404
Call Network API	API Name: bind Args: (c14, 127.0.0.1:49466, 128) Return: 0		2404
Call Network API	API Name: socket Args: (23, 2, 17) Return: c30		2404
Call Network API	API Name: bind Args: (c30, 0.0.0.0:0, 28) Return: 0		2404
Call Network API	API Name: sendto Args: (3120, .y., 34, 0, 1.1.2.254:53, 28) Return: 34		2404
Call Network API	API Name: socket Args: (23, 2, 17) Return: c70		2404
Call Network API	API Name: bind Args: (c70, 0.0.0.0:0, 28) Return: 0		2404
Call Network API	API Name: sendto Args: (3184, .=, 28, 0, 0.0.0.0:5355, 28) Return: 28		2404
Call Network API	API Name: sendto Args: (3184, .=, 28, 0, 224.0.0.252:5355, 28) Return: 28		2404
Call System API	API Name: WinHttpCloseHandle Args: (736144c0) Return: 1		2404
Call Network API	API Name: socket Args: (2, 2, 0) Return: c4c		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: c4c		2404
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003		2404
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: c64		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: c64		2404
Call Network API	API Name: bind Args: (c64, 0.0.0.0:49168, 16) Return: 0		2404
Call System API	API Name: ConnectEx Args: (c64, self.events.data.microsoft.com:443, 16, 0, 0, 0, 735a4998) Return: 0		2404
Call Network API	API Name: send Args: (c64, ..., 1, 191) Return: 0		2404
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		2404
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2404
Call Network API	API Name: sendto Args: (3184, .=, 28, 0, 0.0.0.0:5355, 28) Return: 28		2404
Call Network API	API Name: sendto Args: (3184, .=, 28, 0, 224.0.0.252:5355, 28) Return: 28		2404
Call System API	API Name: WinHttpCloseHandle Args: (736149a0) Return: 1		2404
Call Network API	API Name: socket Args: (23, 1, 6) Return: ebc		2404
Call Network API	API Name: socket Args: (2, 2, 0) Return: f18		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: f18		2404
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2404
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: f20		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: f20		2404
Call Network API	API Name: bind Args: (f20, 0.0.0.0:49169, 128) Return: 0		2404
Call System API	API Name: ConnectEx Args: (f20, ctldl.windowsupdate.com:80, 16, 0, 0, 0, 7028a978) Return: 0		2404
Call Network API	API Name: send Args: (f20, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f460e495f1cc5bb1 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0		2404
Call System API	API Name: WinHttpCloseHandle Args: (78ff6e80) Return: 1		2404
Call System API	API Name: WinHttpCloseHandle Args: (702877e0) Return: 1		2404

Call System API	API Name: WinHttpCloseHandle Args: (78eb3b10) Return: 1		2404
Call Network API	API Name: socket Args: (2, 1, 0) Return: c04		2404
Call Network API	API Name: socket Args: (23, 1, 6) Return: ec0		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\SessionId Value: None		2404
Call System API	API Name: WinHttpCloseHandle Args: (73615ab0) Return: 1		2404
Call Network API	API Name: socket Args: (2, 2, 0) Return: f5c		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: f5c		2404
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87		2404
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: f1c		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: f1c		2404
Call Network API	API Name: bind Args: (f1c, 0.0.0.0:49170, 128) Return: 0		2404
Call System API	API Name: ConnectEx Args: (f1c, gmail.com:443, 16, 0, 0, 0, 7028a978) Return: 0		2404
Call Network API	API Name: send Args: (f1c, ..., 1, 170) Return: 0		2404
Call System API	API Name: WinHttpCloseHandle Args: (794052b0) Return: 1		2404
Call System API	API Name: WinHttpCloseHandle Args: (7028a280) Return: 1		2404
Call Network API	API Name: socket Args: (2, 2, 0) Return: f64		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: f64		2404
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1, 40006000) Return: 87		2404
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1c, 40026000) Return: 9003		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: f64		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: f64		2404
Call Network API	API Name: bind Args: (f64, 0.0.0.0:49171, 128) Return: 0		2404
Call System API	API Name: ConnectEx Args: (f64, autodiscover.gmail.com:443, 16, 0, 0, 0, 70287c18) Return: 0		2404
Call Network API	API Name: send Args: (f64, ..., 1, 183) Return: 0		2404
Call System API	API Name: WinHttpCloseHandle Args: (794027f0) Return: 1		2404
Call System API	API Name: WinHttpCloseHandle Args: (7028a280) Return: 1		2404
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\Program) Return: 1		2404
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2404) Return: 1		2404
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2404
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 1880442320) Return: cc0008		2404
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2022699000, -2067004672, 1880442320) Return: cc000c		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: 758		2404
Call Network API	API Name: bind Args: (758, 0.0.0.0:49172, 16) Return: 0		2404
Call System API	API Name: ConnectEx Args: (758, self.events.data.microsoft.com:443, 16, 0, 0, 0, 735a58e8) Return: 0		2404
Call Network API	API Name: send Args: (758, ..., 1, 191) Return: 0		2404
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII		2404
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CCA5D\1CCA5D Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CCA5D\ Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\!*& Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CE93F\ Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CE93F\1CE93F Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2404\0 Value: None		2404
Call System API	API Name: WinHttpCloseHandle Args: (793f83a0) Return: 1		2404
Call Network API	API Name: socket Args: (2, 2, 0) Return: 1028		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: 1028		2404
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2404
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: f5c		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: f5c		2404
Call Network API	API Name: bind Args: (f5c, 0.0.0.0:49173, 128) Return: 0		2404
Call System API	API Name: ConnectEx Args: (f5c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 79425ed8) Return: 0		2404
Call Network API	API Name: send Args: (f5c, ..., 1, 188) Return: 0		2404
Call System API	API Name: WinHttpCloseHandle Args: (79404f20) Return: 1		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: f5c		2404
Call Network API	API Name: bind Args: (f5c, 0.0.0.0:49174, 128) Return: 0		2404
Call System API	API Name: ConnectEx Args: (f5c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 794248d8) Return: 0		2404
Call Network API	API Name: send Args: (f5c, ..., 1, 188) Return: 0		2404
Call System API	API Name: WinHttpCloseHandle Args: (794040e0) Return: 1		2404
Call System API	API Name: WinHttpCloseHandle Args: (79425c00) Return: 1		2404
Call System API	API Name: WinHttpCloseHandle Args: (79423b00) Return: 1		2404
Call Network API	API Name: socket Args: (2, 2, 0) Return: 1050		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: 1050		2404
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2404
Call System API	API Name: WinHttpCloseHandle Args: (793f7ec0) Return: 1		2404
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2404

Call Network API	API Name: socket Args: (23, 2, 0) Return: 1044		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1044		2404
Call Network API	API Name: bind Args: (1044, 0.0.0.0:49175, 128) Return: 0		2404
Call System API	API Name: ConnectEx Args: (1044, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 79426f58) Return: 0		2404
Call Network API	API Name: send Args: (1044, ..., 1, 188) Return: 0		2404
Call System API	API Name: WinHttpCloseHandle Args: (79403d50) Return: 1		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1044		2404
Call Network API	API Name: bind Args: (1044, 0.0.0.0:49176, 128) Return: 0		2404
Call System API	API Name: ConnectEx Args: (1044, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 79423c78) Return: 0		2404
Call Network API	API Name: send Args: (1044, ..., 1, 188) Return: 0		2404
Call System API	API Name: WinHttpCloseHandle Args: (79404b90) Return: 1		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1044		2404
Call Network API	API Name: bind Args: (1044, 0.0.0.0:49177, 128) Return: 0		2404
Call System API	API Name: ConnectEx Args: (1044, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 79424a38) Return: 0		2404
Call Network API	API Name: send Args: (1044, ..., 1, 188) Return: 0		2404
Call System API	API Name: WinHttpCloseHandle Args: (794032a0) Return: 1		2404
Call System API	API Name: WinHttpCloseHandle Args: (794257e0) Return: 1		2404
Call System API	API Name: WinHttpCloseHandle Args: (79423dc0) Return: 1		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1044		2404
Call Network API	API Name: bind Args: (1044, 0.0.0.0:49178, 128) Return: 0		2404
Call System API	API Name: ConnectEx Args: (1044, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 794270b8) Return: 0		2404
Call Network API	API Name: send Args: (1044, ..., 1, 188) Return: 0		2404
Call System API	API Name: WinHttpCloseHandle Args: (794040e0) Return: 1		2404
Call System API	API Name: WinHttpCloseHandle Args: (79422ea0) Return: 1		2404
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2404
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 2033542208) Return: cc0008		2404
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2022699000, -2067004672, 2033542208) Return: cc000c		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: af8		2404
Call Network API	API Name: bind Args: (af8, 0.0.0.0:49179, 16) Return: 0		2404
Call System API	API Name: ConnectEx Args: (af8, self.events.data.microsoft.com:443, 16, 0, 0, 0, 735ab5a8) Return: 0		2404
Call Network API	API Name: send Args: (af8, ..., 1, 191) Return: 0		2404
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2404
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 2033542208) Return: cc0008		2404
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2022699000, -2067004672, 2033542208) Return: cc000c		2404
Call System API	API Name: WinHttpCloseHandle Args: (793f9c00) Return: 1		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1058		2404
Call Network API	API Name: bind Args: (1058, 0.0.0.0:49180, 16) Return: 0		2404
Call System API	API Name: ConnectEx Args: (1058, self.events.data.microsoft.com:443, 16, 0, 0, 0, 67126498) Return: 0		2404
Call Network API	API Name: send Args: (1058, ..., 1, 191) Return: 0		2404
Call System API	API Name: WinHttpCloseHandle Args: (793f8af0) Return: 1		2404
Call Network API	API Name: socket Args: (2, 2, 0) Return: 1088		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: 1088		2404
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2404
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: 1050		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1050		2404
Call Network API	API Name: bind Args: (1050, 0.0.0.0:49181, 128) Return: 0		2404
Call System API	API Name: ConnectEx Args: (1050, ctldl.windowsupdate.com:80, 16, 0, 0, 0, 79425958) Return: 0		2404
Call Network API	API Name: send Args: (1050, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?40b9a737abd8e0a6 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0		2404
Call System API	API Name: WinHttpCloseHandle Args: (79404b90) Return: 1		2404
Call System API	API Name: WinHttpCloseHandle Args: (79423c60) Return: 1		2404
Call System API	API Name: WinHttpCloseHandle Args: (7013a580) Return: 1		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\File MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\File MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\		2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\User MRU\LiveId_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C495056D56BADD0D4\File MRU\ Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\User MRU\LiveId_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C495056D56BADD0D4\File MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\User MRU\LiveId_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C495056D56BADD0D4\File MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\		2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Place MRU\ Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Place MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Place MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CE93F\1CE93F Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CE93F\ Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ImmersiveWorkbookDirtySentinel Value: 7fffffff		2404
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C4A62860.png Type: VSDT_PNG		2404
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C4A62860.png Type: VSDT_PNG		2404
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C4A62860.png Type: VSDT_PNG		2404
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\6DDB91B.png Type: VSDT_PNG		2404

Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\6DDB91B.png Type: VSDT_PNG		2404
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\6DDB91B.png Type: VSDT_PNG		2404
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\43006102.png Type: VSDT_PNG		2404
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\43006102.png Type: VSDT_PNG		2404
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\43006102.png Type: VSDT_PNG		2404
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\FD4C8D6E.jpeg Type: VSDT_JPG		2404
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\FD4C8D6E.jpeg Type: VSDT_JPG		2404
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\FD4C8D6E.jpeg Type: VSDT_JPG		2404
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\21E64CE1.jpeg Type: VSDT_JPG		2404
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\21E64CE1.jpeg Type: VSDT_JPG		2404
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\21E64CE1.jpeg Type: VSDT_JPG		2404
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2404
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 2027123392) Return: cc0008		2404
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2022699000, -2067004672, 2027123392) Return: cc000c		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: 33c		2404
Call Network API	API Name: bind Args: (33c, 0.0.0.0:49182, 16) Return: 0		2404
Call System API	API Name: ConnectEx Args: (33c, self.events.data.microsoft.com:443, 16, 0, 0, 0, 701badf8) Return: 0		2404
Call Network API	API Name: send Args: (33c, ..., 1, 191) Return: 0		2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2404\0 Value: None		2404
Call System API	API Name: WinHttpCloseHandle Args: (793f8610) Return: 1		2404
Call Network API	API Name: socket Args: (2, 2, 0) Return: b60		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: b60		2404
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2404
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2404
Call Network API	API Name: socket Args: (23, 2, 0) Return: 768		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5a0		2404
Call Network API	API Name: bind Args: (5a0, 0.0.0.0:49183, 128) Return: 0		2404
Call System API	API Name: ConnectEx Args: (5a0, ctldl.windowsupdate.com:80, 16, 0, 0, 0, 70335e18) Return: 0		2404
Call Network API	API Name: send Args: (5a0, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?a60ce6a42bbc3c91 HTTP/1.1\r\nConnection: Keep-Alive\r\n Accept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0		2404
Call System API	API Name: WinHttpCloseHandle Args: (79402b80) Return: 1		2404
Call System API	API Name: WinHttpCloseHandle Args: (702877e0) Return: 1		2404
Call System API	API Name: WinHttpCloseHandle Args: (701399e0) Return: 1		2404
Call Filesystem API	API Name: RemoveDirectoryW Args: (%TEMP%\{74F7DE19-9910-41A3-AA5B-7B698ED9FBAB}\ ) Return: 1		2404
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8F82FDC5.emf) Return: 1		2404
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2404
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 2034627456) Return: cc0008		2404
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2022699000, -2067004672, 2034627456) Return: cc000c		2404
Call Network API	API Name: socket Args: (2, 1, 6) Return: 61c		2404
Call Network API	API Name: bind Args: (61c, 0.0.0.0:49184, 16) Return: 0		2404
Call System API	API Name: ConnectEx Args: (61c, self.events.data.microsoft.com:443, 16, 0, 0, 0, 701c16f8) Return: 0		2404
Call Network API	API Name: send Args: (61c, ..., 1, 191) Return: 0		2404

▼ **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	42F1769E5A244C528AA0660E496FBA7D8B017FCC
SHA-256	258C6B739776F928995E891B7BDB1FD110E3BEBB5BAB8DF96B6344F45A5EB9AB
MD5	F259AF96F465ACA0F7509706778739B0
Size	127542 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
augmentation.osi.office.net	-	53	-	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm
cdn.uci.officeapps.live.com	-	53	-	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm
self.events.data.microsoft.com	-	53	-	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm
ctldl.windowsupdate.com	-	53	-	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm
www.msftncsi.com	-	53	-	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm
gmail.com	-	53	-	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm
autodiscover.gmail.com	-	53	-	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm
autodiscover.gmail.com	-	443	-	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm
gmail.com	-	443	-	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm

URL	Site Category	Risk Level	Threat	Accessed By
https://augmentation.osi.office.net/officeaugmentation/searchendpoint/	Computers / Internet	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm
https://self.events.data.microsoft.com/OneCollector/1.0/	Business / Economy Computers / Internet Cloud Applications	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{358841A5-DBFD-4124-AAEC-D7F3316C54D1}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
winword.exe.db-shm	No risk	-	-	-	32768	D80EE53EC8C1156DB2CE7C8702176F4607E0C232
~$Normal.dotm	No risk	-	-	-	162	CD6FC9530B6A5293D805A7D53F1701220844A3D4
~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx	No risk	-	-	-	162	CB55D282484552F803B9C06C605B5D541552336F
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	302	CB3D8FFD4720B31751307EBE4A7B892452F98172
Word.Settings.json	No risk	-	-	-	87	5281EAE96EFDE7B0E16A1D977F005F0D3BD7AAD0
App_1616237787010322000_A5286CD1-8030-491F-8C28-6B2FCF23ECFC.log	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
Word.CampaignStates.json	No risk	-	-	-	10820	03BF6F8AB1B4E840EF7B17683F47F4C23DFA528A
winword.exe.db-wal	No risk	-	-	-	428512	29321EFAE1F6A9D0538819E61C9537B1C25C5160
Word.SurveyEventActivityStats.json	No risk	-	-	-	14	2FD90B4EC32804DFF7A41B6E63C8B0A40B592113

Analysis

Event Type	Details	Parent PID	PID
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ClientTelemetry\Sampling\0 Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\ Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\"!% Value: None		2416
Delete File	Path: %TEMP%\Diagnostics\WINWORD\App_1600985251099791600_A16BA699-DE8A-473F-B54F-C8D59B3C1D07.log Type: VSDT_EMPTY		2416
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\Diagnostics\WINWORD\App_1600985251099791600_A16BA699-DE8A-473F-B54F-C8D59B3C1D07.log) Return: 1		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2532\0 Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2532\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\ Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\ Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\ Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\ Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\4 Value: 0		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\Categories Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\4 Value: 0		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\Categories Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ULSAllCategories Value: 6, 10		2416
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, 717ef6f0) Return: 0		2416
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 717ef6f0) Return: 0		2416
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 717ef630) Return: 0		2416
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0		2416
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, 717ef630) Return: 0		2416
Call WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0		2416
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, 717ef630) Return: 0		2416

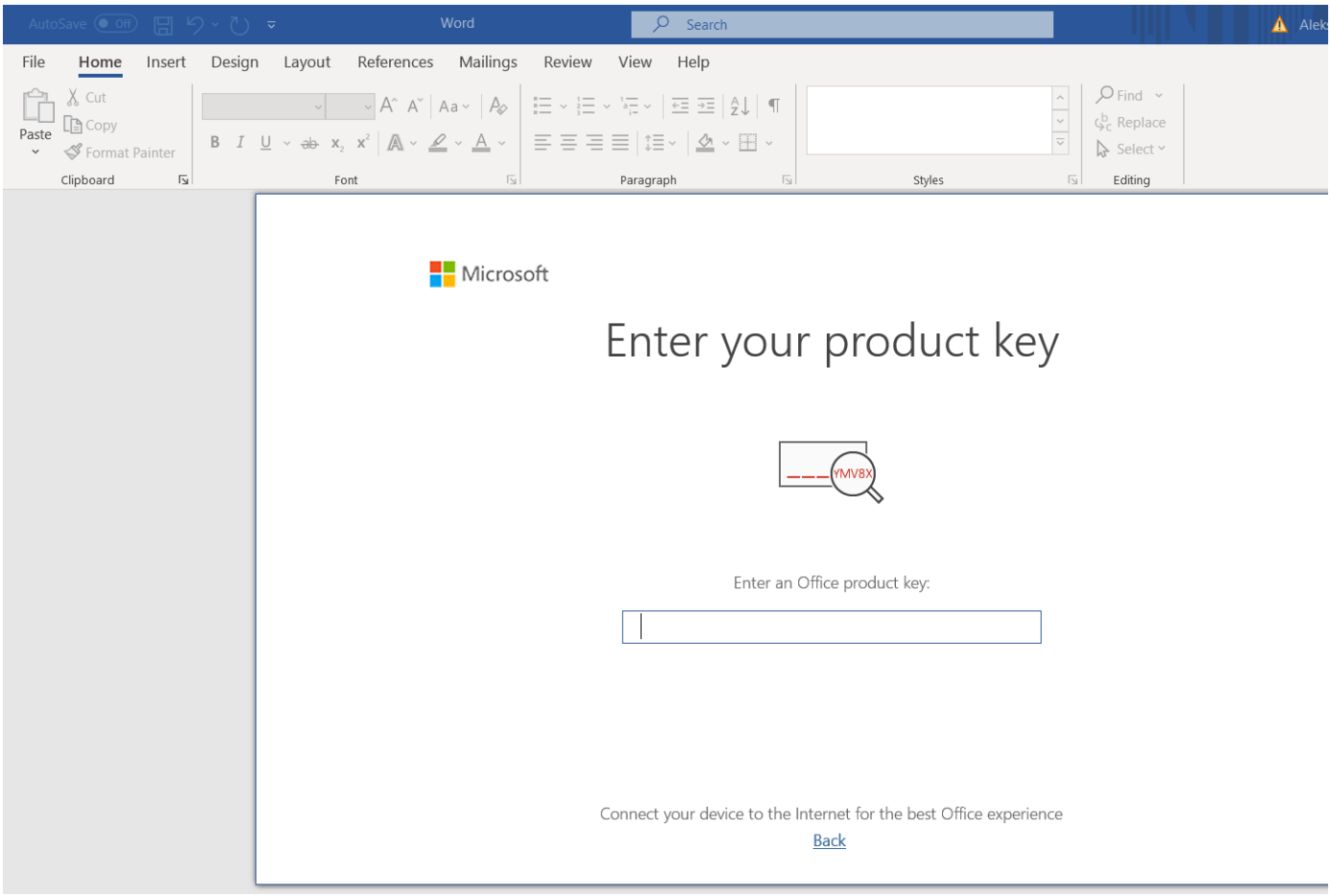
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\f\52C64B7E\LanguageList Value: en-US\0en\0		2416
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, 70dddf40) Return: 0		2416
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 70dddf40) Return: 0		2416
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 70ddde80) Return: 0		2416
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0		2416
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, 70ddde80) Return: 0		2416
Call WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0		2416
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, 70ddde80) Return: 0		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\7x% Value: None		2416
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2416
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\7x% Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastSyncTimeWord Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastWriteTimeWord Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\s{% Value: None		2416
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx) Return: 1		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\s{% Value: None		2416
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\"l% Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\ Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None		2416
Call Network API	API Name: socket Args: (2, 2, 0) Return: 860		2416
Call Network API	API Name: bind Args: (860, 127.0.0.1:61232, 128) Return: 0		2416
Call Network API	API Name: socket Args: (23, 1, 6) Return: ae0		2416
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (717ee590, 0, 0, 0) Return: 1		2416
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0004		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2416
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (717ee430, 0, 0, 0) Return: 1		2416
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (717ee400, 0, 0, 0) Return: 1		2416
Call Network API	API Name: socket Args: (2, 1, 0) Return: a70		2416
Call Network API	API Name: socket Args: (23, 1, 6) Return: b68		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\SessionId Value: None		2416
Call System API	API Name: WinHttpCloseHandle Args: (794a7390) Return: 1		2416
Call Network API	API Name: socket Args: (23, 1, 6) Return: bc0		2416
Call System API	API Name: WinHttpCloseHandle Args: (794a5da0) Return: 1		2416
Call Network API	API Name: socket Args: (2, 2, 0) Return: c30		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: c30		2416
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87		2416
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: c30		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: c30		2416
Call Network API	API Name: bind Args: (c30, 0.0.0.0:49166, 128) Return: 0		2416
Call System API	API Name: ConnectEx Args: (c30, gmail.com:443, 16, 0, 0, 0, 792bc858) Return: 0		2416
Call Network API	API Name: send Args: (c30, ..., 1, 170) Return: 0		2416
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		2416
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2416
Call System API	API Name: WinHttpCloseHandle Args: (69576ed0) Return: 1		2416
Call System API	API Name: WinHttpCloseHandle Args: (792bb240) Return: 1		2416
Call Network API	API Name: socket Args: (2, 2, 0) Return: c30		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: c30		2416
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1, 40006000) Return: 87		2416
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1c, 40026000) Return: 9003		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: c3c		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: c3c		2416
Call Network API	API Name: bind Args: (c3c, 0.0.0.0:49167, 128) Return: 0		2416
Call System API	API Name: ConnectEx Args: (c3c, autodiscover.gmail.com:443, 16, 0, 0, 0, 792bab78) Return: 0		2416
Call Network API	API Name: send Args: (c3c, ..., 1, 183) Return: 0		2416
Call System API	API Name: WinHttpCloseHandle Args: (69953950) Return: 1		2416
Call System API	API Name: WinHttpCloseHandle Args: (792ba060) Return: 1		2416
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2416
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 1922072384) Return: cc0008		2416

Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2061562408, -2067004672, 1922072384) Return: cc000c		2416
Call Network API	API Name: socket Args: (2, 2, 0) Return: e68		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: e68		2416
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87		2416
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: e6c		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: e6c		2416
Call Network API	API Name: bind Args: (e6c, 0.0.0.0:49168, 16) Return: 0		2416
Call System API	API Name: ConnectEx Args: (e6c, self.events.data.microsoft.com:443, 16, 0, 0, 0, 7917ac48) Return: 0		2416
Call Network API	API Name: send Args: (e6c, ..., 1, 191) Return: 0		2416
Call System API	API Name: WinHttpCloseHandle Args: (794a6760) Return: 1		2416
Call Network API	API Name: socket Args: (2, 2, 0) Return: ee0		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: ee0		2416
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2416
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: e64		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: e64		2416
Call Network API	API Name: bind Args: (e64, 0.0.0.0:49169, 128) Return: 0		2416
Call System API	API Name: ConnectEx Args: (e64, ctldl.windowsupdate.com:80, 16, 0, 0, 0, 792ba1d8) Return: 0		2416
Call Network API	API Name: send Args: (e64, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?695643c83cd73052 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0		2416
Call System API	API Name: WinHttpCloseHandle Args: (72d06c30) Return: 1		2416
Call System API	API Name: WinHttpCloseHandle Args: (792ba8a0) Return: 1		2416
Call System API	API Name: WinHttpCloseHandle Args: (728b1e00) Return: 1		2416
Call Network API	API Name: socket Args: (23, 1, 6) Return: ef8		2416
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0008		2416
Call System API	API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003		2416
Call Internet Helper API	API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c		2416
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc000c, GET, /officeaugmentation/searchendpoint/, , , 0, -2134884352, 1994827568) Return: cc0010		2416
Call Network API	API Name: socket Args: (2, 2, 0) Return: f08		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: f08		2416
Call System API	API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 40006000) Return: 87		2416
Call System API	API Name: WinHttpCloseHandle Args: (794a6eb0) Return: 1		2416
Call Network API	API Name: socket Args: (2, 2, 0) Return: f24		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: f24		2416
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2416
Call Network API	API Name: socket Args: (23, 2, 17) Return: f34		2416
Call Network API	API Name: bind Args: (f34, 0.0.0.0:0, 28) Return: 0		2416
Call Network API	API Name: sendto Args: (3892, '.., 45, 0, 1.1.2.254:53, 28) Return: 45		2416
Call System API	API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1c, 40026000) Return: 9003		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: f28		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: f14		2416
Call Network API	API Name: bind Args: (f14, 0.0.0.0:49170, 16) Return: 0		2416
Call System API	API Name: ConnectEx Args: (f14, augmentation.osi.office.net:443, 16, 0, 0, 0, 791731c8) Return: 0		2416
Call Network API	API Name: send Args: (f14, ..., 1, 188) Return: 0		2416
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: f10		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: f10		2416
Call Network API	API Name: bind Args: (f10, 0.0.0.0:49171, 128) Return: 0		2416
Call System API	API Name: ConnectEx Args: (f10, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 792bbeb8) Return: 0		2416
Call Network API	API Name: send Args: (f10, ..., 1, 188) Return: 0		2416
Call System API	API Name: WinHttpCloseHandle Args: (78e78280) Return: 1		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: f10		2416
Call Network API	API Name: bind Args: (f10, 0.0.0.0:49172, 128) Return: 0		2416
Call System API	API Name: ConnectEx Args: (f10, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 7906ade8) Return: 0		2416
Call Network API	API Name: send Args: (f10, ..., 1, 188) Return: 0		2416
Call System API	API Name: WinHttpCloseHandle Args: (69954070) Return: 1		2416
Call System API	API Name: WinHttpCloseHandle Args: (792bc000) Return: 1		2416
Call System API	API Name: WinHttpCloseHandle Args: (792bba80) Return: 1		2416
Call System API	API Name: WinHttpCloseHandle Args: (794a53e0) Return: 1		2416
Call Network API	API Name: socket Args: (2, 2, 0) Return: efc		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: efc		2416
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2416
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: f04		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: f04		2416
Call Network API	API Name: bind Args: (f04, 0.0.0.0:49173, 128) Return: 0		2416
Call System API	API Name: ConnectEx Args: (f04, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 7906b208) Return: 0		2416
Call Network API	API Name: send Args: (f04, ..., 1, 188) Return: 0		2416
Call System API	API Name: WinHttpCloseHandle Args: (69954070) Return: 1		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: f04		2416
Call Network API	API Name: bind Args: (f04, 0.0.0.0:49174, 128) Return: 0		2416

Call System API	API Name: ConnectEx Args: (f04, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 792ba498) Return: 0		2416
Call Network API	API Name: send Args: (f04, ..., 1, 188) Return: 0		2416
Call System API	API Name: WinHttpCloseHandle Args: (69954070) Return: 1		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: f04		2416
Call Network API	API Name: bind Args: (f04, 0.0.0.0:49175, 128) Return: 0		2416
Call System API	API Name: ConnectEx Args: (f04, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 792ba8b8) Return: 0		2416
Call Network API	API Name: send Args: (f04, ..., 1, 188) Return: 0		2416
Call System API	API Name: WinHttpCloseHandle Args: (69954070) Return: 1		2416
Call System API	API Name: WinHttpCloseHandle Args: (792bb240) Return: 1		2416
Call System API	API Name: WinHttpCloseHandle Args: (792bc160) Return: 1		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: f04		2416
Call Network API	API Name: bind Args: (f04, 0.0.0.0:49176, 128) Return: 0		2416
Call System API	API Name: ConnectEx Args: (f04, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 792bb258) Return: 0		2416
Call Network API	API Name: send Args: (f04, ..., 1, 188) Return: 0		2416
Call System API	API Name: WinHttpCloseHandle Args: (69954070) Return: 1		2416
Call System API	API Name: WinHttpCloseHandle Args: (7906af30) Return: 1		2416
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2416
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 1922079008) Return: cc0008		2416
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2061562408, -2067004672, 1922079008) Return: cc000c		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: f24		2416
Call Network API	API Name: bind Args: (f24, 0.0.0.0:49177, 16) Return: 0		2416
Call System API	API Name: ConnectEx Args: (f24, self.events.data.microsoft.com:443, 16, 0, 0, 0, 79176418) Return: 0		2416
Call Network API	API Name: send Args: (f24, ..., 1, 191) Return: 0		2416
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2416
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 1922079008) Return: cc0008		2416
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2061562408, -2067004672, 1922079008) Return: cc000c		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: e94		2416
Call Network API	API Name: bind Args: (e94, 0.0.0.0:49178, 16) Return: 0		2416
Call System API	API Name: ConnectEx Args: (e94, self.events.data.microsoft.com:443, 16, 0, 0, 0, 73016668) Return: 0		2416
Call Network API	API Name: send Args: (e94, ..., 1, 191) Return: 0		2416
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2416
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 1922079008) Return: cc0008		2416
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2061562408, -2067004672, 1922079008) Return: cc000c		2416
Call System API	API Name: WinHttpCloseHandle Args: (794a4f00) Return: 1		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: a40		2416
Call Network API	API Name: bind Args: (a40, 0.0.0.0:49179, 16) Return: 0		2416
Call System API	API Name: ConnectEx Args: (a40, self.events.data.microsoft.com:443, 16, 0, 0, 0, 730181f8) Return: 0		2416
Call Network API	API Name: send Args: (a40, ..., 1, 191) Return: 0		2416
Call System API	API Name: WinHttpCloseHandle Args: (794a42d0) Return: 1		2416
Call Network API	API Name: socket Args: (2, 2, 0) Return: f50		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: f50		2416
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2416
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2416
Call Network API	API Name: socket Args: (23, 2, 0) Return: efc		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: efc		2416
Call Network API	API Name: bind Args: (efc, 0.0.0.0:49180, 128) Return: 0		2416
Call System API	API Name: ConnectEx Args: (efc, ctldl.windowsupdate.com:80, 16, 0, 0, 0, 792bb3b8) Return: 0		2416
Call Network API	API Name: send Args: (efc, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?0082730b4b76fc1b HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0		2416
Call System API	API Name: WinHttpCloseHandle Args: (794bbce0) Return: 1		2416
Call System API	API Name: WinHttpCloseHandle Args: (792bb0e0) Return: 1		2416
Call System API	API Name: WinHttpCloseHandle Args: (728b06c0) Return: 1		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\WordName Value: Word (Unlicensed Product)		2416
Call System API	API Name: CryptGenKey Args: (7955e5a0, 6610, 1, 70ddedb8) Return: 1		2416
Call System API	API Name: CryptExportKey Args: (73016740, 73017620, 1, 0, 0, 70ddedb0) Return: 1		2416
Call System API	API Name: CryptExportKey Args: (73016740, 73017620, 1, 0, 7902bdc0, 70ddedb0) Return: 1		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Toolbars\Settings\Microsoft Word Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Data\Settings Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Options\AppWindowPos Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None		2416
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		2416
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{358841A5-DBFD-4124-AAEC-D7F3316C54D1}.tmp) Return: 1		2416
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None		2416
Call Filesystem API	API Name: RemoveDirectoryW Args: (%TEMP%\{4E8E2B97-D54D-42D5-8581-BD0D039D2C38}\ ) Return: 1		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\ Value: None		2416

Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\5 Value: 0		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\Categories Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\4 Value: 0		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\Categories Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\5 Value: 0		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\Categories Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\4 Value: 0		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\Categories Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\4 Value: 0		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\Categories Value: None		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ULSAllCategories Value: 6, 10		2416
Add File	Path: %TEMP%\Diagnostics\WINWORD\App_1616237787008562900_A5286CD1-8030-491F-8C28-6B2FCF23ECFC.log Type: VSDT_ASCII		2416
Write File	Path: %TEMP%\Diagnostics\WINWORD\App_1616237787008562900_A5286CD1-8030-491F-8C28-6B2FCF23ECFC.log Type: VSDT_ASCII		2416
Add File	Path: %TEMP%\Diagnostics\WINWORD\App_1616237787010322000_A5286CD1-8030-491F-8C28-6B2FCF23ECFC.log Type: VSDT_EMPTY		2416
Write File	Path: %TEMP%\Diagnostics\WINWORD\App_1616237787010322000_A5286CD1-8030-491F-8C28-6B2FCF23ECFC.log Type: VSDT_EMPTY		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Licensing\BootTimeSkuOverride\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Licensing\BootTimeSkuOverride\{DC5CCACD-A7AC-4FD3-9F70-9454B5DE5161} Value: {D7279DD0-E175-49FE-A623-8FC2FC00AFC4}		2416
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2416
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 1770995072) Return: cc0008		2416
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2061562408, -2067004672, 1770995072) Return: cc000c		2416
Call Network API	API Name: socket Args: (2, 1, 6) Return: 958		2416
Call Network API	API Name: bind Args: (958, 0.0.0.0:49181, 16) Return: 0		2416
Call System API	API Name: ConnectEx Args: (958, self.events.data.microsoft.com:443, 16, 0, 0, 0, 73018b98) Return: 0		2416
Call Network API	API Name: send Args: (958, ..., 1, 191) Return: 0		2416
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\winword.exe.db-shm) Return: 1		2416
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\winword.exe.db-wal) Return: 1		2416
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{A5286CD1-8030-491F-8C28-6B2FCF23ECFC} - OProcSessId.dat) Return: 1		2416
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2416\ Value: None		2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2416\0 Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None		2416
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\ Value: None		2416

▼ **Screenshot**



Process Graph Legend