Virtual Analyzer Report



Submission Context

Logged	2021-03-20 12:47:51
Submitter	Manual Submission
Туре	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	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	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

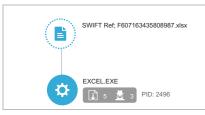
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	TROJ_FRS.0NA103C821		
Exploited vulnerabilities			
Network connection	No network		

▼ 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	1F75301B260414396ABB7790F63B47E5CCDC216CBA57D9B2195CBDA926230EF D
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

 $\ensuremath{\texttt{©}}$ ATT&CKTM is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

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

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 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		0.0.0.049182
Listens on port		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		0.0.0.049176
Listens on port		0.0.0.0:49175
Listens on port		0.0.0.049174
Listens on port		127.0.0.1:61707
Listens on port		0.0.0.049173
Listens on port		0.0.0.0:49172
Listens on port		0.0.0.049171
Listens on port		0.0.0.0:49170
Listens on port		0.0.0.049169
Listens on port		0.0.0.0:49168
Listens on port		0.0.0.49167
Listens on port		0.0.0.0:49166

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
Domain	II Addices	1 011	Location	Trisk Ecvei	Till Cat	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/OneCollect	Business / Economy	No risk	-	SWIFT Ref; F607163435808987.xlsx
or/1.0/	Computers / Internet			
	Cloud Applications			

▼ 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	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

Туре	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		
Maita Danista Mari	Malware Pattern Version: 16.605.92		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Clien\Telemetry\Sampling\1 Value: None		
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\Exce\Resiliency\Startup\tems\ Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Resiliency\Startup\tems\oi& Value: None		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Nmmersive\Workbook\Dirty\Sentine\Value: 0		2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Nexce\Nexce\WorkbookOpenedCount Value: 0		2496
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\Diagnostics\EXCEL\App_1600985250979406400_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, edab/290) 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\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\Roaming\LastSyncTimeExcel Value: None		2496

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLast\WriteTimeExcel 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\Exce\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\Exce\Resillency\DocumentRecovery\ Value: None	2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\1CBB88\ Value: None	2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\1CBB88\1CBB88 Value: None	2496
Call System API	API Name: CryptDeriveKey Args: (eeb93d20, 660e, 11f13d90, 800000, e3a289e0) Return: 1	2496
Call System API	API Name: CryptDeriveKey Args: (eeb93d20, 660e, 11f0f720, 800000, f1ddab28) Return: 1	2496
Call System API	API Name: CryptDeriveKey Args: (eeb93d20, 660e, 11f0ea00, 800000, 11ddab28) 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: (110e290, 0, 0, 0, e3a28d88, 10.) Return: 1	2496
Call System API	API Name: BCryptDecrypt Args: (11ec6430, Sir?»", 32, 0, , 0, Sir?»", 32, -475886256, 0) Return: 0	2496
Call System API		2496
	API Name: CryptDecrypt Args: (f1f0e290, 0, 0, 0, f1e966b0, 20) Return: 1	
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: (flec6430, , 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\Exce\Nexce\N	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ¾ ¥"Ĭ, 4096, 0, , 0, ¾ ¥"Ĭ, 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: (11f0e290, 0, 0, 0, 11eebd0c, 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~ÝŮ[í¼¯Öku5²™ Ű\rÃ, 4096, 0, , 0, ì~ÝŨ[í¼¯Öku5²™ Ű\rÃ, 4096, -475896800, 0) Return: 0	2496
Call System API	API Name: CryptDecrypt Args: (11f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, PD, 4096, 0, , 0, PD, 4096, -475896800, 0) Return: 0	2496
Call System API	API Name: CryptDecrypt Args: (110e290, 0, 0, 0, 11eebd0c, 1000) Return: 1	2496
Call System API	API Name: BCryptDecrypt Args: (11ec6430, ø51~ûq, 4096, 0, , 0, ø51~ûq, 4096, -475896800, 0) Return: 0	2496
•	API Name: CryptDecrypt Args: (11f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1	
Call System API		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, īnN, 4096, 0, , 0, īnN, 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, 'Úi, 4096, 0, , 0, 'Úi, 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: (flec6430, , 3296, 0, , 0, , 3296, -475897872, 0) Return: 0	2496
Call System API	API Name: CryptDecrypt Args: (110e290, 0, 0, 0, 11eebd0c, ce0) Return: 1	2496
Call System API	API Name: BCryptDecrypt Args. (11ec6430, PK, 4096, 0, , 0, PK, 4096, -475896496, 0) Return: 0	2496
Call System API	API Name: CryptDecrypt Args. (11f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1	2496
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CBB88\1CBB88 Value: None	2496
Write Registry Key Call System API		
Call System API	API Name: BCryptDecrypt Args: (flec6430, , 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: (11f0e290, 0, 0, 0, f1eebd0c, 1000) Return: 1	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, 'Úi, 4096, 0, , 0, 'Úi, 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, -qCEg, 4096, 0, , 0, -qCEg, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ä´¶ xªQĹñĨĬĬQ¹, 4096, 0, , 0, ä´¶ xªQĹñĨĬĬQ¹, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, É;tœÒĐg ×¶fÃc-™?³,Pà‡æfÐ, 4096, 0, , 0, É;tœÒĐg ×¶fÃc-™?³,Pà‡æfÐ, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ÏCü²èäe†]¡Ù'€Îž "Z,tã2, 4096, 0, , 0, ÏCü²èäe†]¡Ù'€Ĩž "Z,tã2, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, \r<\pi_4096, 0, , 0, \r<\pi_4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, `8öñiÆôV©³¢§'š, 4096, 0, , 0, `8öñiÆôV©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: (flec6430, , 4096, 0, , 0, , 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ÉÂÇ1Y^, 4096, 0, 1, 0, ÉÂÇ1Y^, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, 2/D£ÖuÔ†\rlf,9'52,"ŒÜÁP[k H±, 4096, 0, 0, 2/D£ÖuÔ†\rlf,9'52,"ŒÜÁP[k H±, 4096, -475902688, 0) Return: 0	2496
Can Cyclom AFT	API Name: BCryptDecrypt Args: (11ec6430, 2(DE0U0T\rift,952, 'EUAP K H±, 4096, 0, 0, 0, 2(DE0U0T\rift,952, 'EUAP K H±, 4096, -475902688, 0) Return: 0 API Name: BCryptDecrypt Args: (11ec6430, , 4096, 0, 0, 0, 4096, -475902688, 0) Return: 0	2496
Call System API		∠ 4 30
Call System API Call System API	API Name: BCryptDecrypt Args: (11ec6430, [9+//E,Žžodî, 4096, 0, 1, 0, [9+//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'_Úf'ø'¢ZÈÀV, 4096, 0, , 0, q'_Úf'ø'¢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, £";"Y, 4096, 0, , 0, £";"Y, 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, å, 4096, 0, , 0, å, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (11ec6430, ½, %, %, %, %, %, %, %, %, %, %, %, %, %,	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)t‡ZÊ,š®āi¿&)=fpÅ82™, 4096, 0, 0, æí)t‡ZÊ,š®āi¿&)=fpÅ82™, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, %!ĒóŮ]7T\¤, 4096, 0, , 0, %!ĒóÙ]7T\¤, 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 Å'Ž»cž, 4096, 0, , 0, ØñEÔ Å'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, ĂA"ñ-wwÁwuTbÔl, 4096, 0, , 0, ĂA"ñ-wwÁwuTbÔl, 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, ō?Ñ]WsyaÂBû»/€Ài0ÎHÀ,ưó^h′p, 4096, 0, , 0, ō?Ñ]WsyaÂBû»/€Ài0ÎHÀ,ưó^h′p, 4096, -475902688, 0) Return	2496
	: 0	
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, f1¥'ØÇÑ×~Þ¯hèlv'½Un, 4096, 0, , 0, f1¥'ØÇÑ×~Þ¯hèlv'½Un, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ¬bWa÷"äÖ, 4096, 0, , 0, ¬bWa÷"äÖ, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ôÞ)rüQn2ÈbRi, 4096, 0, , 0, ôÞ)rüQn2ÈbRi, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (11ec6430, (", 4096, 0, , 0, (", 4096, 475902688, 0) Return: 0	2496
•		
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Yg, 4096, 0, 10, Yg, 4096, 475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, -wΰ˰Nỹ‰ê¤, 4096, 0, 0, -wΰ˰Nỹ‰ê¤, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, +i)èg, 4096, 0, , 0, +i)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, =އ)C¬óÑ‹\rÏݽò,¡ÜrÄbç \nÒôw#þÊ:i", 4096, 0, , 0, =އ)C¬óÑ‹\rĨݽò,¡ÜrÄbç \nÒôw#þÊ:i", 4096, -475902688, 0	2496
) Return: 0	
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 3*âÜ1Ŏ-H_0D%)k, %*7[, 4096, 0, , 0, ¼, a 3*âÜ1Ō-H_0D%)k, %*7[, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, :é8Ózißàu, 4096, 0, , 0, :é8Ózißàu, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, dÖl´1¢Êfμ,èl, 4096, 0, , 0, dÖl´1¢Êfμ,èl, 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©3ÿXûj*84¯ĺó¾v, 4096, 0, , 0, ¶×;2©3ÿXûj*84¯ĺó¾v, 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, Ûīy¨òg73Ó91^Û öt{ñRC¼Ôè*èzJ, 4096, 0, , 0, Ûīy¨òg73Ó91^Û öt{ñRC¼Ôè*èzJ, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ŎÚ(÷I, 4096, 0, , 0, ŌÚ(÷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, 10, ë), 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, èl'xĺØ]ı@), 4096, 0, , 0, èl'xĺØ]ı@), 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, *[æ'{û±(-bi€ÕOj, 4096, 0, , 0, *]æ'{û±(-bi€ÕOj, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, §g' u¡}u±/ō, 4096, 0, , 0, §g' u¡}u±/ō, 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, êË¿, 4096, 0, , 0, êË¿, 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, É, 4096, 0, , 0, É, 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¯ΥχὄΡο°£^"δΥ, 4096, 0, , 0, [μ¯ΥχὄΡο°£^"δΥ, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, š'ö¯\¿Þ ÄUxDÔ—Ô*S¤7—òi,Lùèл%ô@, 4096, 0, , 0, š'ö¯\¿Þ ÄUxDÔ—Ô*S¤7—òi,Lùèл%ô@, 4096, -475902	2496
	688, 0) Return: 0	
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-i, 4096, 0, , 0, (2-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, 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,½Z"¿, 4096, 0, , 0, 3ùQ,½Z"¿, 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: (11ec0430,24, 4096, 0, , 0,24, 4096, -475902688, 0) Return: 0	2496
		2496
Call System ADI	API Name: BCryptDecrypt Args: (f1ec6430, ĐfCE*, 4096, 0, , 0, ĐfCE*, 4096, -475902688, 0) Return: 0	
Call System API	ADI Nama P.Caust Decarat Assau / f1cc6420 Stret / 4006 C 0 Sec. 1/40000 A75000000 O Detroit	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ä¤x½, 4096, 0, , 0, ä¤x½, 4096, -475902688, 0) Return: 0	
Call System API Call System API	API Name: BCryptDecrypt Args: (f1ec6430, , 4096, 0, , 0, , 4096, -475902688, 0) Return: 0	2496
Call System API		

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 ^Ái½m, 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, Oo, 4096, 0, , 0, Oo, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, ½®òjfk, 4096, 0, , 0, ½®òjfk, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, 8ùùôā»/×0ý/Åq, 4096, 0, , 0, 8ùùôā»/×0ý/Åq, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, 'H'iΣG²Ô, 4096, 0, , 0, 'H'iΣG²Ô, 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Ý, ••WZÙ#Đu\$èXb*Ôf½í ¥ō™a½níW=3?DìÌÓ‡ć**, 4096, 0, , 0, Ý, ••WZÙ#Đu\$èXb*Ôf½í ¥ō™a½níW=3?DìÌÓ‡ć**, 4	2496
Call System Art	096, -475902688, 0) Return: 0	2430
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}û¯Ú, 4096, 0, , 0, "ayü\l}û¯Ú, 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: (flec6430, °lr~, 4096, 0, 0, °lr~, 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, Ŏi\$AöæÄâty ñ+¼ōGžæºl̃3, 4096, 0, , 0, Ōi\$AöæÄâty ñ+¼ōGžæºl̃3, 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: (11ec6430, žóěÁ¢´1., 4096, 0, , 0, žóěÁ¢´1., 4096, -475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (flec6430, érM, 4096, 0, 0, érM, 4096, 475902688, 0) Return: 0	2496
Call System API	API Name: BCryptDecrypt Args: (f1ec6430, Ù"æ—Ūööu, 4096, 0, , 0, Ù"æ—Ūööu, 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	$Key: HKEY_CURRENT_USER \\ \label{linear} Software \\ \label{linear} Microsoft \\ \label{linear} Windows \\ \label{linear} Current \\ \label{linear} Version \\ \label{linear} Interversion \\ \label{linear} Version \\ line$	2496
Delete Registry Key	$Key: HKEY_CURRENT_USER \label{linear} Is Software \label{linear} Windows \label{linear} Current \label{linear} Version \label{linear} Internet Settings \label{linear} Proxy Override \label{linear} Version \labelle \labelle \labelle \labelle \labelle \labelle \labelle \labe$	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\Current\Version\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		2496
·	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2496) Return: 1	
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, 0.0.0.49166, 16) Return: 0	2496
		2400
Detection	Threat Characteristic: Listens on port 0.0.0.049166	
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
		2496
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	2430
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Val	2496
	ue: None	
Call System API	API Name: WinHttpCloseHandle Args: (f1efb450) Return: 1	2496
	API Name: socket Args: (23, 1, 6) Return: d98	2496
Call Network API	74 Thans. Society age. (25, 1, 6) Telanii aso	2496
Call Network API Call Network API	API Name: socket Args: (2, 2, 0) Return: df4	
	API Name: socket Args: (2, 2, 0) Return: df4	2496
Call Network API Call Network API	API Name: socket Args: (2, 2, 0) Return: df4 API Name: socket Args: (23, 2, 0) Return: df4	
Call Network API Call Network API Call System API	API Name: socket Args: (2, 2, 0) Return: df4 API Name: socket Args: (23, 2, 0) Return: df4 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87	2496
Call Network API Call Network API Call System API Call System API	API Name: socket Args: (2, 2, 0) Return: df4 API Name: socket Args: (23, 2, 0) Return: df4 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003	2496 2496
Call Network API Call Network API Call System API Call System API Call Network API	API Name: socket Args: (2, 2, 0) Return: df4 API Name: socket Args: (23, 2, 0) Return: df4 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d88	2496 2496 2496
Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API	API Name: socket Args: (2, 2, 0) Return: df4 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d88 API Name: socket Args: (2, 1, 6) Return: d88	2496 2496 2496 2496
Call Network API Call Network API Call System API Call System API Call Network API	API Name: socket Args: (2, 2, 0) Return: df4 API Name: socket Args: (23, 2, 0) Return: df4 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d88	2496 2496 2496
Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API	API Name: socket Args: (2, 2, 0) Return: df4 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003 API Name: socket Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d88 API Name: socket Args: (2, 1, 6) Return: d88 API Name: bind Args: (d88, 0.0.0.049167, 128) Return: 0 Threat Characteristic: Listens on port	2496 2496 2496 2496
Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call Network API Detection	API Name: socket Args: (2, 2, 0) Return: df4 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003 API Name: socket Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d88 API Name: socket Args: (2, 1, 6) Return: d88 API Name: bind Args: (d88, 0.0.0.049167, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.049167	2496 2496 2496 2496 2496
Call Network API Call System API Call System API Call System API Call Network API Call Network API Call Network API Call Network API	API Name: socket Args: (2, 2, 0) Return: df4 API Name: socket Args: (23, 2, 0) Return: df4 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d88 API Name: socket Args: (2, 1, 6) Return: d88 API Name: socket Args: (d88, 0.0.0.049167, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.49167 API Name: ConnectEx Args: (d88, ctldl.windowsupdate.com:80, 16, 0, 0, 0, f1f3b958) Return: 0	2496 2496 2496 2496
Call Network API Call System API Call System API Call System API Call Network API Call Network API Call Network API Detection	API Name: socket Args: (2, 2, 0) Return: df4 API Name: socket Args: (23, 2, 0) Return: df4 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d88 API Name: socket Args: (2, 1, 6) Return: d88 API Name: socket Args: (2, 1, 6) Return: d88 API Name: bind Args: (d88, 0.0.0.49167, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.49167 API Name: ConnectEx Args: (d88, ctldl.windowsupdate.com:80, 16, 0, 0, 0, 11f3b958) Return: 0 API Name: send Args: (d88, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?64ddc54b9581b1b6 HTTP/1.1\nnConnection: Keep-Alive\n/1	2496 2496 2496 2496 2496
Call Network API Call Network API Call System API Call System API Call Network API Call System API	API Name: socket Args: (2, 2, 0) Return: df4 API Name: socket Args: (23, 2, 0) Return: df4 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d88 API Name: socket Args: (2, 1, 6) Return: d88 API Name: socket Args: (d88, 0.0.0.049167, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.49167 API Name: ConnectEx Args: (d88, ctldl.windowsupdate.com:80, 16, 0, 0, 0, f1f3b958) Return: 0	2496 2496 2496 2496 2496 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, 11f3b3d8) 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 Contain ADI		0400
Call System API	API Name: ConnectEx Args: (df4, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 11f3c198) 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: (11f3afa0) 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	
	0.0.0.949170	
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	2100
Detection	0.0.0.049171	
Call System API	API Name: ConnectEx Args: (e24, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 11f3b538) 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
		2430
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, 11f3b958) 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: (122e)040) Return: 1	2496
Call System API	API Name: WinHttpCloseHandle Args: (1f13b100) 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		2496
	API Name: ConnectEx Args: (e24, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, f1f3b538) Return: 0	
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: (11f38d40) 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	127.0.0.1:61707 Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII	2496
	127.0.0.1:61707 Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII	2496 2496
Add File	127.0.0.1:61707 Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII	
Add File Write File	127.0.0.1:61707 Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII	2496
Add File Write File Delete Registry Key	127.0.0.1:61707 Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CBB88\1CBB88 Value: None	2496 2496
Add File Write File Delete Registry Key Delete Registry Key	127.0.0.1:61707 Path: %LOCALAPPDATA%\Microsoft\Office\16.0\WeftCustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII Path: %LOCALAPPDATA%\Microsoft\Office\16.0\WeftCustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\1CBB88\1CBB88 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\1CBB88\Value: None	2496 2496 2496
Add File Write File Delete Registry Key Delete Registry Key Delete Registry Key	127.0.0.1:61707 Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Resiliency\Document\Recovery\1CBB88\1CBB88 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Resiliency\Document\Recovery\1CBB88\Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Resiliency\Document\Recovery\Value: None	2496 2496 2496 2496
Add File Write File Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	127.0.0.1:61707 Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CBB88\1CBB88 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CBB88\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2496 2496 2496 2496 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\Exce\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, 0.0.0.49174, 128) Return: 0	2496
Detection	Threat Characteristic: Listens on port 0.0.0.49174	
Call System API	API Name: ConnectEx Args: (103c, gmail.com:443, 16, 0, 0, 0, 66ea7118) Return: 0	2496
Call Network API	API Name: send Args: (103c,, 1, 170) Return: 0	2496
Call System API	API Name: WinHttpCloseHandle Args: (170dade0) Return: 1	2496
Call System API	API Name: WinHttpCloseHandle Args: (16ea5840) 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	
	0.0.0.049175	
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	
	0.0.0.49176	
Call System API	API Name: ConnectEx Args: (102c, self.events.data.microsoft.com:443, 16, 0, 0, 0, 16693b48) 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, 0.0.0.49177, 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, 16e96708) 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\Exce\File MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\	2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\File MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\	2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\User MRU\Liveld_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C4950	2496
	56D56BADD0D4\File MRU\ Value: None	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\User MRU\Liveld_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C4950	2496
Write Registry Key	56D56BADD0D4\File MRU\FOLDERIID_Desktop Value: %USERPROFILE%\Desktop\ Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\10\ser MRU\Liveld_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C4950	2496
	56D56BADD0D4\File MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\	
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Place MRU\ Value: None	2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Place MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\	2496
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\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
	API Name: socket Args: (2, 1, 6) Return: 1034	2496
Call Network API		2496
Call Network API Call Network API	API Name: bind Args: (1034, 0.0.0.49178, 16) Return: 0	
	Threat Characteristic: Listens on port	
Call Network API Detection	Threat Characteristic: Listens on port 0.0.0.0:49178	2406
Call Network API	Threat Characteristic: Listens on port	2496 2496

Call System API	API Name: WinHttpCloseHandle Args: (f6e437c0) Return: 1	2496
Call Network API Call Network API	API Name: socket Args: (2, 2, 0) Return: 1060 API Name: socket Args: (23, 2, 0) Return: 1060	2496 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	
Call System API	0.0.0.049179 ADI Namor ConnectEv Avec / e29, ettal windowsundets com 00, 45, 0, 0, 0 (foot 400). Return 0	2496
Call Network API	API Name: ConnectEx Args: (e38, ctdl.windowsupdate.com:80, 16, 0, 0, 0, 16ae5498) Return: 0 API Name: send Args: (e38, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f8d25b66fe4dab7a HTTP/1.1\f\nConnection: Keep-Alive\r\n	2496
Can Notificial I	Accept: */"\n\User-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0	
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\Current\Version\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 API Name: DeleteFile\W Area: / % \ OCA\ APDDATA\\Microsoft\Sebamae\MS Event restart vm\ \ \ Pature: 0	2496
Call Filesystem API Write Registry Key	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Schemas\MS Excel_restart.xml) Return: 0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\\9B92EB61-CBC1-11D3-8C2	2496 2496
vinc regions res	Key: HKEY_LOCAL_MACHINE\SOFTWARE\MicrosoftOffice\ClickTokunike\cisTrY\MACHINE\SOFTWARE\Classes\TypeLib\{\98992EB61-CBC1-11D3-8C2} D-00A0CC37B591\}\1.2\(\text{Default}\) Value: Microsoft Smart Tags 2.0 Type Library	2450
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-	2496
W . D	A27D-11D3-BD33-D80C46980A07}\ Value: None	0.400
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\{3C6C0440-1000}	2496
	A27D-11D3-BD33-D80C46980A07}\(Default) Value: None	
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432\Node\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-	2496
	A27D-11D3-BD33-D80C46980A07}\ProxyStubClsid32\(Default) Value: None	
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-	2496
	A27D-11D3-BD33-D80C46980A07)\TypeLib\(Default)\Value: None	
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-	2496
	A27D-11D3-BD33-D80C46980A07}\TypeLib\Version Value: 1.2	
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-	2496
white registry rey	B735-11D3-B2CF-00500489D6A3)\(Default) Value: None	2430
Write Registry Key	$Key: HKEY_LOCAL_MACHINE \\ SOFTWARE: Microsoft \\ Office \\ Click \\ To Run \\ REGISTRY \\ MACHINE \\ SOFTWARE: Classes \\ Wow 6432 \\ Node \\ Interface \\ \{9BF068D0-100000000000000000000000000000000000$	2496
	B735-11D3-B2CF-00500489D6A3)(Default) Value: None	0.400
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\Proxy\StubClsid32\tValue: None	2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-	2496
	B735-11D3-B2CF-00500489D6A3\ProxyStubClsid32\(Default\) Value: None	
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-	2496
	B735-11D3-B2CF-00500489D6A3}\TypeLib\ Value: None	
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-	2496
	B735-11D3-B2CF-00500489D6A3)\TypeLib\(Default)\Value:\None	
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-C	2496
· · · · · · · · · · · · · · · · · · ·	DD7-11D3-B2D4-00500489D6A3}\ Value: None	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-C	2496
Write Registry Key	DD7-11D3-B2D4-00500489D6A3)\(Default) Value: None Kav: HKEV LOCAL MACHINELSOFTMARE\(Microsoft)\(Office\)ClickToRun\(REG\)STRVMACHINELSOFTMARE\(Classes\)Wnw6432Node\(latertare\)J54E37842.C	2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-C DD7-11D3-B2D4-00500489D6A3}\(Default\) Value: None	2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-C	2496
Weita Register V.	DD7-11D3-B2D4-00500489D6A3}\ProxyStubClsid32\Value: None	2406
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-C DD7-11D3-B2D4-00500489D6A3}\ProxyStubClsid32\(Default\) Value: None	2496
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-C	2496
Write Registry Key		
Add Registry Key	DD7-11D3-B2D4-00500489D6A3}\ProxyStubClsid32\(Default\) Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-C	2496

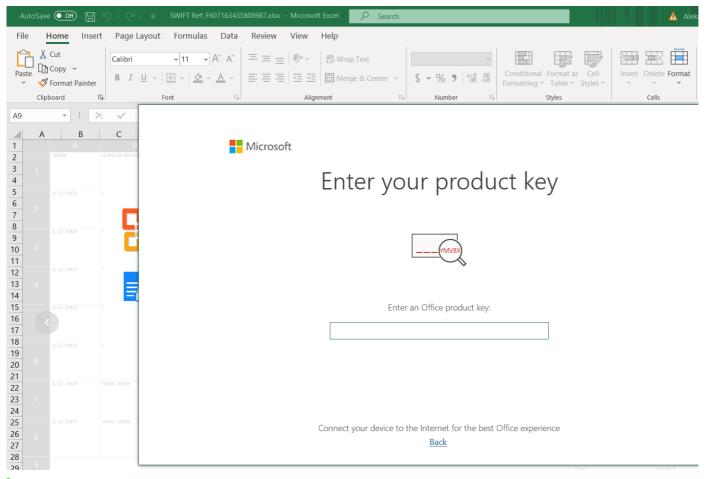
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432\Node\Interface\(54F37842-C) DD7-11D3-B2D4-00500489D6A3\)\TypeLib\(Default\) Value: None	2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(54F37842-C) DD7-11D3-B2D4-00500489D6A3\)\TypeLib\(Default)\ Value: None	2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-C DD7-11D3-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\{38744D8F-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\(38744D8F-B8A5-11D3-B2CF-00500489D6A3\)\ProxyStubClsid32\\Value: None	2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{38744D8F-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\(38744D8F-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\{38744D8F-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\{38744D8F-B8A5-11D3-B2CF-00500489D6A3\}Type\Lib\(\text{Default}\) Value: None	2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(38744D8F-B8A5-1103-B2CF-00500489D6A3\)TypeLib\Version Value: 1.2	2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\\Wow6432Node\Interface\{D4C62D17-	2496
Write Registry Key	6162-41DE-BE24-5B1D3F529CC3)\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE:\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\[D4C62D17-]	2496
Write Registry Key	6162-41DE-BE24-5B1D3F529CC3)\(Default) Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\(Microsoft\)Office\ClickToRun\(REGISTRY\)MACHINE\SOFTWARE\(Classes\)\(Wow6432\)Node\(Interface\)\(D4C62D17-	2496
Add Registry Key	6162-41DE-BE24-5B1D3F529CC3)\(Default) Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\(Microsoft\)Office\(ClickToRun\)\(REGISTRY\)MACHINE\SOFTWARE\(Classes\)\(Wow6432\)Node\(Interface\)\([0.4C62D17-1]\)	2496
Write Registry Key	6162-41DE-BE24-5B1D3F529CC3}\ProxyStubClsid32\Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432\Node\Interface\{D4C62D17-	2496
Write Registry Key	6162-41DE-BE24-5B1D3F529CC3)\ProxyStubClsid32\(\text{Oefault}\)\Value:\None Key:\HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\Office\ClickToRun\\REGISTRY\MACHINE\SOFTWARE\Classes\\Wow6432\Node\Interface\\\D4C62D17-	2496
Add Registry Key	6162-41DE-BE24-5B1D3F529CC3)\Proxy\StubClsid32\(\text{Default}\)\Value:\None Key:\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432\Node\Interface\{\D4C62D17-	2496
Write Registry Key	6162-41DE-BE24-5B1D3F529CC3)TypeLib\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432\Node\Interface\{\Data}\Data\ClickToRun\REGISTRY\MACHINE\SOFTWARE\(\Data\)	2496
	6162-41DE-BE24-5B1D3F529CC3}\TypeLib\(Default\) Value: None	
Write Registry Key	Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432\Node\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\Wow6432\Node\Interface\(\{\gamma}\)BF068D0-B736-11D3-B2CF-00500489D6A4\\(\gamma\)(Default)\Value: None	2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(\{\gamma}\)BF068D0-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-0050048906A4\}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-005004890B6A5\}\(Default\) 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\\Proxy\\$tubClsid32\\Notate:\None	2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{\9BF068D0-	2496
Write Registry Key	B736-11D3-B2CF-00500489D6A5)\ProxyStubClsid32\(Default\) Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(\graphi\)9BF068D0-	2496
Add Registry Key	B736-11D3-B2CF-00500489D6A5}\ProxyStubClsid32\(\text{Default}\) Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(\gamma\)9BF068D0-	2496
Write Registry Key	B736-11D3-B2CF-00500489D6A5)\TypeLib\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{\9BF068D0-	2496
Write Registry Key	B736-11D3-B2CF-00500489D6A5)\TypeLib\(Default\) Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(\grace\)9BF068D0-	2496
Write Registry Key	B736-11D3-B2CF-00500489D6A5)\TypeLib\(Default)\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{\9BF068D0-	2496
Add Registry Key	B736-11D3-B2CF-00500489D6A5}\TypeLib\Version Value: 1.2 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{\9BF068D0-	2496
Write Registry Key	B736-11D3-B2CF-00500489D6A6}\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{\9BF068D0-	2496
	B736-11D3-B2CF-00500489D6A6}\(Default)\(Value:\(None\)	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(\gamma\)68D0-B736-11D3-B2CF-00500489D6A6}\(\Qmathred\(\gamma\)\(\gamma\)1D3-B2CF-00500489D6A6}\(\Qmathred\(\gamma\)\(\gamma\)\(\gamma\)\(\gamma\)\(\gamma\)	2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{\gammaBF068D0-B736-11D3-B2CF-00500489D6A6\\Proxy\StubClsid32\\Value: None	2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(\gamma\)9BF068D0-B736-11D3-B2CF-00500489D6A6\(\gamma\)ProxyStubClsid32\(\gamma\)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\(\text{Default}\) 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\}\Type\Lib\(\text{Default}\) 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\}\Type\Lib\Version\Value: 1.2	2496
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(\){5073BDEB-E480-4024-4887E-22923X004444}\) Value: None	2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(5073BDEB-1000)	2496
Write Registry Key	E480-4024-887E-22923C004444)\(Default)\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\(Microsoft\)Office\ClickToRun\REGISTRY\(MACHINE\SOFTWARE\)Classes\(Wow6432\)Node\(\lambda\)Interface\(\lambda\)5073BDEB-	2496
Call System API	E480-4024-887E-22923C004444)(Default) Value: None 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\) \(\) \	2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(\){5073BDEB-E480-4024-887E-22923C004444\(\)\Proxy5\tube\Clsid32\(\)(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\Wow6432\Node\Interface\(\){5073BDEB-E480-4024-887E-22923C004444}\ProxyStubCisid32\(\)(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\ClickToRum\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\(\frac{5073BDEB-E480-4024-887E-22923C004444}\)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-8771-14FB705547AE}\(Default\) 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-	2496
Write Registry Key	6CE8-449F-87F1-1AFB705547AE])ProxyStubClsid32\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\MicrosoftOffice\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(FE6A04A8-0000000000000000000000000000000000	2496
Write Registry Key	6CE8-449F-87F1-1AFB705547AE)\ProxyStubClsid32\(Default\) Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(FE6A04A8-\)	2496
Call Network API	6CE8-449F-87F1-1AFB705547AE)\ProxyStubClsid32\(Default\) Value: None 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-	2496
Call Network API	6CE8-449F-87F1-1AFB705547AE)\TypeLib\ Value: None API Name: bind Args: (9b8, 0.0.0.049180, 16) Return: 0	2496
	Threat Characteristic: Listens on port	

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\Wow6432\Node\Interface\{FE6A04A8-	2496
Write Registry Key	6CE8-449F-87F1-1AFB705547AE):TypeLib\(Default\) Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\(Microsoft\)Office\(ClickToRun\)REGISTRY\(MACHINE\SOFTWARE\(Classes\)\Wow6432Node\(lnterface\)\((FE6A04A8-1) \)	2496
Add Registry Key	6CE8-449F-87F1-1AFB705547AE);TypeLib\Version Value: 1.2 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\(\frac{1}{9}\)BF068D0-	2496
	B736-11D3-B2CF-00500489D6D6}\ Value: None	
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}\Proxy\StubClsid32\(Default\) Value: None	2496
Call System API	API Name: ConnectEx Args: (9b8, self.events.data.microsoft.com:443, 16, 0, 0, 0, 16e99178) 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-00500489B6D6\)TypeLib\(Default\) Value: None	2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\\(\graphi = 0.0000000000000000000000000000000000	2496
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{\gammaBF068D0-	2496
Add Pagistay Koy	B736-11D3-B2CF-00500489D6D6)\TypeLib\Version Value: 1.2 Kay: HKEY_CLIDENT_LISED\Schware\Microschildricesc	2496
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\ Value: None	
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\XLMA\N\FriendlyName Value: Microsoft Excel	2496
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMA\N\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\Exce\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\\NetCache\Content.MSO\\992A98E0.png Type: VSDT_PNG	2496
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\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%IMicrosoftWindowsIINetCachelContent.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\\NetCache\Content.MSO\87744B9B.png Type: VSDT_PNG	2496
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\\NetCache\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\NetCache\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\NetCache\Content.MSO\9EF57D17.jpeg Type: VSDT_JPG	
	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\FD28D1EE.jpeg Type: VSDT_JPG	2496
Add File	r aut. /vcconcnrrunt/giviiotosottivviiidowstitivetoachetoutileiit.ivisot/ruzou rec.jpeg rype. vsbr.jdPG	490
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INatCache\Conton MCO\ED28D1EE inon Tuno; VSST_IDC	2496
Add File Write File Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\FD28D1EE.jpeg Type: VSDT_JPG Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\FD28D1EE.jpeg Type: VSDT_JPG	2496 2496

Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2496 File: %LOCALAPPDATA%\Microsoft\Windows\\NetCache\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, 66e94ef8) 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, 16aec818) Return: 0	2496
Call Network API	API Name: send Args: (6a0, GET /msdownload/update/v3/static/trustedr/en/disallowedcertsll.cab?9aa4e523a84d64eb HTTP/1.1lvlnConnection: Keep-Alive\n nAccept: */"\n\u00fcsep-Agent: Microsoft-CryptoAPI/6.3\n\u00e4holst: ctldl.windowsupdate.com\n\u00e4n\u00e4n\u00e4n, 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	49CB1E34DB1EDC4F45178E1F7DA9EEB4B79112F41A16684E100E107842B3604
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/OneCollect or/1.0/	Business / Economy Computers / Internet	No risk	-	NONAMEFL
	Cloud Applications			

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
excel.exe.db-shm	No risk	-	-	-	32768	D4F87270D99C1B3CFD83FA16358FDD400F 79050F
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
excel.exe.db-wal	No risk	-	-	-	4152	FE9AEFBCC9EAA3154B13965A64473821C1 DBF459
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	302	64468F3F568586DB742F3908FC13A079196 BE298
App_1616237907177800100_187 28FC5-2DD3-4F90-BBDB-9CA7C 1B51E0A.log	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
8F82FDC5.emf	No risk	-	-	-	653280	333C8CD569694A103E049EC626C173C9AA 5673D0
6DDB91B.png	No risk	-	-	-	51166	85B228BBC80DC60D40F4D3473E10B742E7 B9039E
{18728FC5-2DD3-4F90-BBDB-9C A7C1B51E0A} - OProcSessId.dat	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
43006102.png	No risk	-	-	-	79394	9F3FE15AE44644F9ED8C2CA668B7020DF7 26426B
App_1616237907173854200_187 28FC5-2DD3-4F90-BBDB-9CA7C 1B51E0A.log	No risk	-	-	-	16694	6DCA62FF92E7321ED6B78195602744A7CB 74456B

▼ 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\Excel\WorkbookOpenedCount 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, 6/2ff5d0) 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) R eturn: 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\f\62C64B7E\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

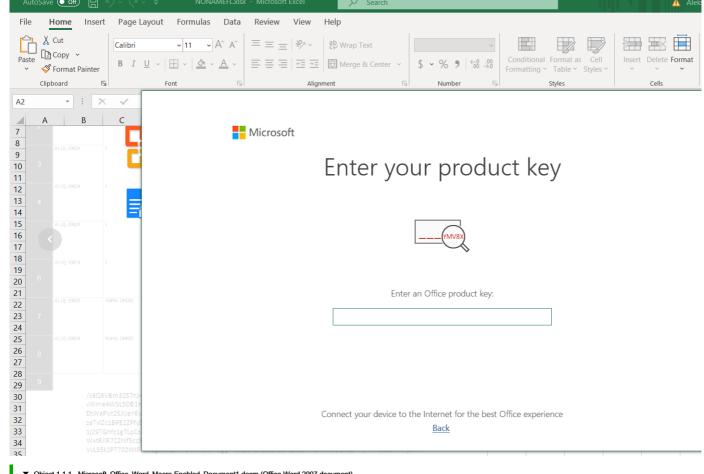
Call WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0	2404
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, 6f83e000) Return: 0	2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None	2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\Roaming\LastSyncTimeExcel Value: None	2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\Roaming\LastWriteTimeExcel Value: None	2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\Startupltems\&% 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\Exce\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\Current\Version\Internet Settings\ProxyServer Value: None	2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyOverride Value: None	2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\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\Current\Version\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\Exce\Resiliency\DocumentRecovery\1CCA5D\1CCA5D Value: None	2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Excel\Excel\Delta okOpenedCount 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, 0.0.0:5355, 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: N one	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, 0.0.0.5355, 28) Return: 28	2404
Call Network API	API Name: sendio 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: 118	2404
Call System API	API Name: DnsQueryEx Args: (ctidl.windowsupdate.com, 1, 40006000) Return: 87	2404
Call System API	API Name: DnsQueryEx Args: (ctdl.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
	API Name: bind Args: (f20, 0.0.0.49169, 128) Return: 0	2404
Call Network API		2404
Call Network API Call System API	API Name; ConnectEx Args; (TzU, ctig), windowsundate.com:80. Tb. 0. 0. 0. 70289978 1 Return: 0	
Call System API	API Name: ConnectEx Args: (f20, ctldl.windowsupdate.com:80, 16, 0, 0, 0, 7028a978) Return: 0 API Name: send Ards: (f20, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f460e495f1cc5bb1 HTTP/1.1\r/nConnection: Keep-Alive\r/nA	2404
	API Name: ConnectEx Args: (120, ctidi.windowsupdate.com:su, 16, 0, 0, 1, 1028a978) Return: 0 API Name: send Args: (120, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab97460e495f1cc5bb1 HTTP/1.1\n\nConnection: Keep-Alive\nA ccept: */"\nUser-Agent: Microsoft-CryptoAPI/6.3\n\nHost: ctldl.windowsupdate.com\n\n\n, 1, 201) Return: 0	2404
Call System API	API Name: send Args: (†20, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f460e495f1cc5bb1 HTTP/1.1\r\nConnection: Keep-Aliveir\nA	2404

An Interest Principal Content An Interest Principal Conten			
Milliams Milliams	Call System API	API Name: WinHttpCloseHandle Args: (78eb3b10) Return: 1	2404
Month Mont	Call Network API	API Name: socket Args: (2, 1, 0) Return: c04	2404
March Marc	Call Network API	API Name: socket Args: (23, 1, 6) Return: ec0	2404
APPROXIMATION APPROXIMATIO	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\SessionId Value: None	2404
Miller M	Call System API	API Name: WinHttpCloseHandle Args: (73615ab0) Return: 1	2404
Add	Call Network API	API Name: socket Args: (2, 2, 0) Return: f5c	2404
	Call Network API		2404
Beta	Call System API		2404
Marie Marie (Parl Million State (Parl 1,000 Million From Parl Million			
March Marc			
50 日本日の日本日			
日本日の中の日で、			
A	Call Network API	API Name: bind Args: (11c, 0.0.0.0:49170, 128) Return: 0	
Mary March March	Call System API	API Name: ConnectEx Args: (11c, gmail.com:443, 16, 0, 0, 0, 7028a978) Return: 0	2404
An International Content	Call Network API	API Name: send Args: (f1c,, 1, 170) Return: 0	2404
March Art	Call System API	API Name: WinHttpCloseHandle Args: (794052b0) Return: 1	2404
Description All All New Secritor (April (2015) (1) Nature 18 364	Call System API	API Name: WinHttpCloseHandle Args: (7028a280) Return: 1	2404
Miles Mile	Call Network API	API Name: socket Args: (2, 2, 0) Return: f64	2404
50 5000 70 70 70 70 70 7	Call Network API	API Name: socket Args: (23, 2, 0) Return: f64	2404
Marchard PA	Call System API		2404
Marchan APT			
APP Marce APP APP APP Marce School (port 16, 16 Relain Ed 16 App Marce 16 App			
Antique			
APT APT			
APP APP	Call Network API	API Name: bind Args: (f64, 0.0.0.0:49171, 128) Return: 0	
AP Name Wirth (Contention of Age 12 and 12 and 12 and 12 and 13 and	Call System API	API Name: ConnectEx Args: (f64, autodiscover.gmail.com:443, 16, 0, 0, 0, 70287c18) Return: 0	2404
APT Part P	Call Network API	API Name: send Args: (f64,, 1, 183) Return: 0	2404
API Name Continue Rough API Name Continue Rough (a)	Call System API	API Name: WinHttpCloseHandle Args: (794027f0) Return: 1	2404
Cell Specim API	Call System API	API Name: WinHttpCloseHandle Args: (7028a280) Return: 1	2404
APT Description APT APT Description of the profit			2404
Call Spriss (PI			
Call Internet Negley APR			
Call Internet Helpo API			
Call Network API			
Call System APT	· · · · · · · · · · · · · · · · · · ·		
Call Spalent AF	Call Network API	API Name: socket Args: (2, 1, 6) Return: 758	2404
Call Nation's API	Call Network API	API Name: bind Args: (758, 0.0.0.0:49172, 16) Return: 0	2404
Add File	Call System API	API Name: ConnectEx Args: (758, self.events.data.microsoft.com:443, 16, 0, 0, 0, 735a58e8) Return: 0	2404
Vehic Path No. COLLAPPEAT AN Microsoft Office (16 (Weh Custom Functionary) 1.79 to sprogrames part Type: VBDT / ASCII 2444 Debate Registry Key	Call Network API	API Name: send Args: (758,, 1, 191) Return: 0	2404
Debies Registy Key	Add File	Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII	2404
Debiets Registry Key	Write File	Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII	2404
Debiets Registry Key	Delete Registry Key		2404
Delete Regility Key			
Debite Registry Key			
Deiest Ragistry Key			
Delete Registry Key			
Add Registry Key Key: HKEY_CURRENT_USERS/Software/Microsoft/Office16 OfficeoRealistancy/Dourser/Recovery/Value: None 2404		,	
Add Registry Key	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2404
Add Registy Key	Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2404
Write Registry Kery Key: HKEY_CURRENT_USERS/oftware/Microsoft/Office 16. 0/ExceRealilency/DocumentRecovery/1CE9SF\1CE9SF\1CE9SF\1ce9SF\1ce3EV\1c	Add Registry Key	$Key: HKEY_CURRENT_USER \\ \label{eq:locality} ISCALL \\ \label{eq:locality} White \\ \l$	2404
Write Registry Key Key; HKEY_CURRENT_USERSoftware/Microsoft/Office/Common/CrashPersistence/EXCEL/24040 Value: None 2404 Call System API API Name: WinHttpClose/Handle Args: (738/830) Return: 1028 2404 Call Network API API Name: socket Args: (2, 2, 0) Return: 1028 2404 Call System API API Name: booket Args: (23, 2, 0) Return: 1028 2404 Call System API API Name: Challey/Exik Args: (cdn.ucl. officeapps live.com, 1, 40026000) Return: 87 2404 Call System API API Name: Socket Args: (23, 2, 0) Return: 15c 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 15c 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 15c 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 15c 2404 Call Network API API Name: bind Args: (15c, 0, 0, 0, 049173, 128) Return: 0 2404 Call System API API Name: send Args: (15c, 0, 0, 0, 049173, 128) Return: 0 2404 Call Network API API Name: send Args: (15c, 0, 0, 0, 049173, 128) Return: 0 2404 Call Network API API Name: send Args: (15c, 0, 0, 0, 049174, 128) Return: 0 2404 Call Network API API Name: winHttpCloseHandle Args: (7940420)	Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CE93F\ Value: None	2404
Call System API API Name: WinHttpCloseHandle Args: (79383a0) Return: 1 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 1028 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 1028 2404 Call System API API Name: DnsCueryEx Args: (coth uci-officeapps.live.com, 1, 40006000) Return: 87 2404 Call System API API Name: DnsCueryEx Args: (coth uci-officeapps.live.com, 1, 40006000) Return: 903 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 15c 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 15c 2404 Call Network API API Name: socket Args: (25, 0, 0, 0, 49173, 128) Return: 0 2404 Call Network API API Name: Socket Args: (5c, 0, 00, 0, 0, 49173, 128) Return: 0 2404 Call System API API Name: socket Args: (5c, 0, 00, 0, 0, 49174, 128) Return: 0 2404 Call System API API Name: socket Args: (5c, 0, 00, 0, 49174, 128) Return: 0 2404 Call System API API Name: socket Args: (2, 1, 6) Return: 16c 2404 Call Network API API Name: socket Args: (5c, 0, 00, 0, 49174, 128) Return: 0 2404 Call Network API API Name: socket Args: (5c, 00, 00, 49174,	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CE93F\1CE93F\1CE93F\value: None	2404
Call System API API Name: WinHttpCloseHandle Args: (79383a0) Return: 1 2404 Call Network API API Name: socket Args: (23, 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 2204 Call Network API API Name: socket Args: (23, 2, 0) Return: 15c 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 15c 2404 Call Network API API Name: socket Args: (25, 0, 0.00.49173, 128) Return: 0 2404 Call Network API API Name: socket Args: (15c, 0.00.0.49173, 128) Return: 0 2404 Call System API API Name: socket Args: (15c, 0.00.0.49174, 128) Return: 0 2404 Call System API API Name: socket Args: (21, 16) Return: 15c 2404 Call System API API Name: socket Args: (21, 16) Return: 15c 2404 Call Network API API Name: socket Args: (21, 16) Return: 15c 2404 Call Network API API Name: socket Args: (15c, 0.00.0.49174, 128) Return: 0 2404		Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2404\0 Value: None	
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, 4006600) 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: 15c 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 5c 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 0 2404 Call Network API API Name: socket Args: (5c, 00.00.49173, 128) Return: 0 2404 Call System API API Name: send Args: (5c, 00.00.49173, 128) Return: 0 2404 Call System API API Name: send Args: (5c, 00.00.49174, 128) Return: 0 2404 Call System API API Name: socket Args: (7.9404120) Return: 1 2404 Call Network API API Name: socket Args: (7.5c, 00.00.49174, 128) Return: 0 2404 Call System API API Name: socket Args: (7.5c, 00.00.049174, 128) Return: 0 2404 Call System API API Name: WinttipCloseHandle Args: (79404200) Return: 1 2404			
Call Network API API Name: socket Args: (23, 2, 0) Return: 1028 2404 Call System API API Name: DnsQueryEx Args: (20, 10.ci.officeapps.live.com, 1, 40006000) Return: 87 2404 Call System API API Name: DnsQueryEx Args: (20, 32, 0) Return: 156 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 156 2404 Call Network API API Name: socket Args: (2, 1, 6) Return: 156 2404 Call Network API API Name: bind Args: (15c, 0.00.049173, 128) Return: 0 2404 Call System API API Name: connectEx Args: (15c, cot.nuci.officeapps.live.com:443, 16, 0, 0, 0, 79425ed8) Return: 0 2404 Call System API API Name: socket Args: (2, 1, 6) Return: 15 2404 Call System API API Name: winHttpcCloseHendle Args: (75c, od.nuci.officeapps.live.com:443, 16, 0, 0, 0, 79425ed8) Return: 0 2404 Call Network API API Name: socket Args: (2, 1, 6) Return: 15c 2404 Call Network API API Name: socket Args: (2, 1, 6) Return: 16c 2404 Call Network API API Name: socket Args: (2, 1, 6) Return: 16 2404 Call System API API Name: connectEx Args: (5c, od.nuci.officeapps.live.com:443, 16, 0, 0, 0, 794248d8) Return: 0 2404 Call System API	·		
Call System API API Name: DnsQueryEx Args: (odn.uci.officeapps.live.com, 1, 40006000) Return: 97 2404 Call System API API Name: DnsQueryEx Args: (odn.uci.officeapps.live.com, 1c, 40026000) Return: 9003 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 15c 2404 Call Network API API Name: socket Args: (22, 1, 6) Return: 15c 2404 Call Network API API Name: bind Args: (15c, 0, 0.0.049173, 128) Return: 0 2404 Call System API API Name: bind Args: (15c, 0, 0.0.049173, 128) Return: 0 2404 Call System API API Name: send Args: (15c, 0.0.0.049174, 128) Return: 0 2404 Call Network API API Name: send Args: (15c, 0.0.0.049174, 128) Return: 1 2404 Call Network API API Name: socket Args: (23, 1, 6) Return: 15c 2404 Call Network API API Name: bind Args: (15c, 0.0.0.049174, 128) Return: 0 2404 Call System API API Name: bind Args: (15c, 0.0.0.049174, 128) Return: 0 2404 Call System API API Name: bind Args: (15c, 0.0.0.049174, 128) Return: 0 2404 Call System API API Name: send Args: (15c, 0.0.0.049174, 128) Return: 0 2404 Call System API API Name: send Args: (15c, 0.0.0.049174, 128) Re			
Call System API API Name: DinsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 15c 2404 Call Network API API Name: bind Args: (15c, 0, 0, 0, 0:49173, 128) Return: 0 2404 Call Network API API Name: bind Args: (15c, 0, 0, 0, 0:49173, 128) Return: 0 2404 Call System API API Name: connectEx Args: (15c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 79425ed8) Return: 0 2404 Call Network API API Name: send Args: (15c,, 1, 188) Return: 0 2404 Call System API API Name: withittpCloseHandle Args: (79404020) Return: 1 2404 Call Network API API Name: bind Args: (15c, 0, 0, 0. 0:49174, 128) Return: 0 2404 Call Network API API Name: bind Args: (15c, 0, 0. 0. 0:49174, 128) Return: 0 2404 Call System API API Name: ConnectEx Args: (15c, 0. o. 0. 0:49174, 128) Return: 0 2404 Call System API API Name: WinHttpCloseHandle Args: (7940402) Return: 1 2404 Call System API API Name: WinHttpCloseHandle Args: (7940402) Return: 1 2404 Call System API API Name: WinHttpCloseHandle Args: (7940402) Return: 1 2404 Call System API API Name: WinHttpCloseHandle Args: (7942500) Return: 1 <			
Call Network API API Name: socket Args: (23, 2, 0) Return: 15c 2404 Call Network API API Name: socket Args: (21, 16) Return: 15c 2404 Call Network API API Name: bind Args: (15c, 0.0.0.049173, 128) Return: 0 2404 Call System API API Name: ConnectEx Args: (15c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 79425ed8) Return: 0 2404 Call Network API API Name: send Args: (15c,, 1, 188) Return: 0 2404 Call System API API Name: winHttpCloseHandle Args: (79404f20) Return: 1 2404 Call Network API API Name: socket Args: (15c, 0.0.0.0.49174, 128) Return: 0 2404 Call Network API API Name: socket Args: (15c, 0.0.0.0.49174, 128) Return: 0 2404 Call System API API Name: connectEx Args: (15c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 794248d8) Return: 0 2404 Call Network API API Name: send Args: (15c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 794248d8) Return: 0 2404 Call Network API API Name: send Args: (15c,, 1, 188) Return: 0 2404 Call System API API Name: winHttpCloseHandle Args: (79425c00) Return: 1 2404 Call System API API Name: winHttpCloseHandle Args: (79425b00) Return: 1 2404 Call Netwo			
Call Network API API Name: socket Args: (2, 1, 6) Return: f5c 2404 Call Network API API Name: bind Args: (f5c, 00.00.49173, 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: 5c 2404 Call Network API API Name: bind Args: (f5c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 794248d8) 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, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 794248d8) Return: 0 2404 Call System API API Name: send Args: (f5c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 794248d8) Return: 0 2404 Call System API API Name: WinHttpCloseHandle Args: (794040e0) Return: 1 2404 Call System API API Name: WinHttpCloseHandle Args: (7942500) Return: 1 2404 Call Network API API Name: socket Args: (2, 2, 0) Return: 1050 2404 Call Network API			
Call Network API API Name: bind Args: (15c, 0.0.0.0:49173, 128) Return: 0 2404 Call System API API Name: ConnectEx Args: (15c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 79425ed8) Return: 0 2404 Call Network API API Name: send Args: (15c,, 1, 188) Return: 0 2404 Call System API API Name: WinHttpCloseHandle Args: (79404f20) Return: 1 2404 Call Network API API Name: socket Args: (21, 6) Return: 15c 2404 Call Network API API Name: bind Args: (15c, 0.0.0.0.49174, 128) Return: 0 2404 Call System API API Name: connectEx Args: (15c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 794248d8) Return: 0 2404 Call Network API API Name: send Args: (15c,, 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: (22, 0) Return: 1050 2404 Call Network API API Name: socket Args: (23, 2, 0) Return: 1050 2404 Call System API API Name: socket Args: (23, 2, 0) Return: 1050 2404 Cal	Call Network API	API Name: socket Args: (23, 2, 0) Return: f5c	2404
Call System API API Name: ConnectEx Args: (15c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 79425ed8) Return: 0 2404 Call Network API API Name: send Args: (15c,, 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: 15c 2404 Call Network API API Name: bind Args: (15c, 0.0.0.0:49174, 128) Return: 0 2404 Call System API API Name: ConnectEx Args: (15c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 794248d8) Return: 0 2404 Call Network API API Name: send Args: (15c,, 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: (79425c00) 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: socket Args: (23, 2, 0) Return: 1050 2404 Call System API API Name: socket Args: (23, 2, 0) Retur	Call Network API	API Name: socket Args: (2, 1, 6) Return: f5c	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: (15c, 0.0.0.049174, 128) Return: 0 2404 Call System API API Name: ConnectEx Args: (15c, cd.n.uci.officeapps.live.com:443, 16, 0, 0, 0, 794248d8) Return: 0 2404 Call Network API API Name: send Args: (15c,, 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: (79425c00) 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: 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 Network API	API Name: bind Args: (f5c, 0.0.0.0:49173, 128) 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, 0.0.0.049174, 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: 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: ConnectEx Args: (f5c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 79425ed8) Return: 0	2404
Call Network API API Name: socket Args: (2, 1, 6) Return: f5c 2404 Call Network API API Name: bind Args: (f5c, 0.0.0.049174, 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: (794040e) Return: 1 2404 Call System API API Name: WinHttpCloseHandle Args: (7942500) Return: 1 2404 Call System API API Name: WinHttpCloseHandle Args: (79423b00) 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 Network API	API Name: send Args: (f5c,, 1, 188) Return: 0	2404
Call Network API API Name: socket Args: (2, 1, 6) Return: 15c 2404 Call Network API API Name: bind Args: (15c, 0.0.0.049174, 128) Return: 0 2404 Call System API API Name: ConnectEx Args: (15c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 794248d8) Return: 0 2404 Call Network API API Name: send Args: (15c,, 1, 188) Return: 0 2404 Call System API API Name: WinHttpCloseHandle Args: (794040e) 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 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 Network API API Name: bind Args: (f5c, 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: (794040e) Return: 1 2404 Call System API API Name: WinHttpCloseHandle Args: (7942500) Return: 1 2404 Call System API API Name: WinHttpCloseHandle Args: (79423000) Return: 1 2404 Call System API API Name: WinHttpCloseHandle Args: (79423000) 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: 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, cdn.uci.officeapps.live.com, 1, 188) Return: 0 2404 Call System API API Name: WinHttpCloseHandle Args: (794040e0) Return: 1 2404 Call System API API Name: WinHttpCloseHandle Args: (7942500) 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 Network API API Name: send Args: (f5c,, 1, 188) Return: 0 2404 Call System API API Name: WinHttpCloseHandle Args: (794040e)) Return: 1 2404 Call System API API Name: WinHttpCloseHandle Args: (7942500) 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: (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: (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: (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: (794040e0) 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: (79425c00) Return: 1	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: (79423b00) Return: 1	2404
Call System API API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87 2404	Call Network API	API Name: socket Args: (2, 2, 0) Return: 1050	2404
Call System API API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87 2404	Call Network API	API Name: socket Args: (23, 2, 0) Return: 1050	2404
2404			
Call System API API Name: DnsQueryEx Args; (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003 2404			
Call System API API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003	Odii Oystelli Ar I	A Trianic. Dissada yez Argo. (windonoinoapponiva.wini, 10, 400/2000) / Retuini. 8000	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
		2404
Call System API	API Name: ConnectEx Args: (af8, self.events.data.microsoft.com:443, 16, 0, 0, 0, 735ab5a8) Return: 0	
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: (793/9c00) 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, 0.0.0:49181, 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\n\connection: Keep-Alive\r\n\accept: "\"\n\u00fasep: \"\"\n\u00fasep-Alive\r\u00fasep: \"\"\n\u00fasep: \"\"\n\u00fasep: \"\"\n\u00fasep: \"\"\n\u00fasep: \\u00fasep: \u00fasep: \\u00fasep: \\u00fa	2404
Call System ADI		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\Exce\File MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\	2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\File MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\	2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\User MRU\Liveld_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C4950 56D56BADD0D4\File MRU\ Value: None	2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\User MRU\Liveld_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C4950 56D56BADD0D4\File MRU\FOLDER\D_Desktop Value: %USERPROFILE\Desktop\	2404
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\User MRU\Live\d_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C4950 56D56BADD0D4\File MRU\FOLDERID_Documents \square\live\userboxer\underb	2404
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\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\Exce\Place MRU\FOLDER\D_Documents Value: %USERPROFILE%\Documents\	2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Resiliency\Document\Recovery\1CE93\F1\CE93F\1Ce93F\1Ce9\Resiliency\Document\Recovery\1CE93\F1\CE93F\1Ce9	2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Resiliency\Document\Recovery\1CE93F\1CE93F\ Value: None	2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Resiliency\DocumentRecovery\ Value: None	2404
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Exce\Resiliency\ Value: None	2404
=	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ImmersiveWorkbookDirtySentinel Value: 7fffffff	2404
Write Registry Key		
Write Registry Key Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C4A62860.png Type: VSDT_PNG	2404
	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C4A62860.png Type: VSDT_PNG Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C4A62860.png Type: VSDT_PNG	2404
Add File		

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%iMicrosoftlWindowsliNetCache\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-CryptoAPif6.3\r\nHost: ctidl.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: (70207/e0) Return: 1 API Name: WinHttpCloseHandle Args: (701399e0) Return: 1	2404
Call System API	API Name: winntipcloserianole Args: (70139960) Return: 1 API Name: RemoveDirectoryW Args: (%TEMP%\(774F7DE19-9910-41A3-AA5B-7B698ED9FBAB\\)) Return: 1	2404
· · · · · · · · · · · · · · · · · · ·		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Windows\\NetCache\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	258C6B739776F928995E891B7BDB1FD110E3BEBB5BAB8DF96B6344F45A5EB9A
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/OneCollect or/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-AA EC-D7F3316C54D1}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86 E49677
winword.exe.db-shm	No risk	-	-	-	32768	D80EE53EC8C1156DB2CE7C8702176F4607 E0C232
~\$Normal.dotm	No risk	-	-	-	162	CD6FC9530B6A5293D805A7D53F170122084 4A3D4
~\$crosoft_Office_Word_Macro-En abled_Document1.docm.docx	No risk	-	-	-	162	CB55D282484552F803B9C06C605B5D54155 2336F
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	302	CB3D8FFD4720B31751307EBE4A7B892452 F98172
Word.Settings.json	No risk	-	-	-	87	5281EAE96EFDE7B0E16A1D977F005F0D3B D7AAD0
App_1616237787010322000_A52 86CD1-8030-491F-8C28-6B2FCF 23ECFC.log	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
Word.CampaignStates.json	No risk	-	-	-	10820	03BF6F8AB1B4E840EF7B17683F47F4C23D FA528A
winword.exe.db-wal	No risk	-	-	-	428512	29321EFAE1F6A9D0538819E61C9537B1C25 C5160
Word.SurveyEventActivityStats.js on	No risk	-	-	-	14	2FD90B4EC32804DFF7A41B6E63C8B0A40B 592113

▼ Analysis

Event Type	Details	Parent PID	PID
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ClientTelemetry\Sampling\0 Value: None		2416
ld Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\ Value: None		2416
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None		2416
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2416
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2416
ld Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\ Value: None		2416
ld Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\ Value: None		2416
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\1\% Value: None		2416
elete File	Path: %TEMP%IDiagnostics\WINWORD\App_1600985251099791600_A16BA699-DE8A-473F-B54F-C8D59B3C1D07.log Type: VSDT_EMPTY		2416
all Filesystem API	API Name: DeleteFileW Args: (%TEMP%/Diagnostics\WINWORD\App_1600985251099791600_A16BA699-DE8A-473F-B54F-C8D59B3C1D07.log) Return: 1		2416
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2532\0 Value: None		2416
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2532\ Value: None		2416
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None		2416
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93 A0-2BC6273BC8E4}\ Value: None		2416
elete 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
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2 C8-4E80CAEA5B07}\ Value: None		2416
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-8 1B2-FEA7244F6FFA}\ Value: None		2416
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562B88E-422D-4B5C-B20E-90D710F7D11C}\Value: None		2416
lete Registry Key	$Key: HKEY_CURRENT_USER \\ \label{localized} Software \\ \label{localized} Microsoft \\ \label{localized} Of ficel \\ 16.0 \\ \label{localized} Common \\ \label{localized} Client \\ \label{localized} Telemetry \\ \label{localized} Rules \\ \mbox{Metadatal winword.exe} \\ \mbox{ETWMonitor } Value: None \\ \mbox{Metadatal winword.exe} \\ \mbox{The localized } Telemetry \\ \mbox{Rules Metadatal winword.exe} \\ \mbox{The localized } Telemetry \\ \mbox{Rules Metadatal winword.exe} \\ \mbox{The localized } Telemetry \\ \mbox{Rules Metadatal winword.exe} \\ \mbox{The localized } Telemetry \\ The $		2416
lete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2416
lete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2416
d Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2416
d Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2416
ld 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
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562B88E-422D-4B5C-B20E-90D710F7D11C}\4 Value: 0		2416
/rite 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
dd Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93 A0-2BC6273BC8E4}\ Value: None		2416
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93 A0-2BC6273BC8E4}\4 Value: 0		2416
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\(02FD33DF-F746-4A10-93 A0-2BC6273BC8E4\)\Categories Value: None		2416
ld Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\Value: None		2416
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ULSAllCategories Value: 6, 10		2416
II WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, 717ef6f0) Return: 0		2416
II WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 717ef6f0) Return: 0		2416
II WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 717ef630) Return: 0		2416
II WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0		2416
all WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE "%PHYSICALDRIVE0%", 30, 0, 717ef630) Return: 0		2416
all WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0		2416
all WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag=*Physical Memory 0*, 30, 0, 717ef630) Return: 0		2416

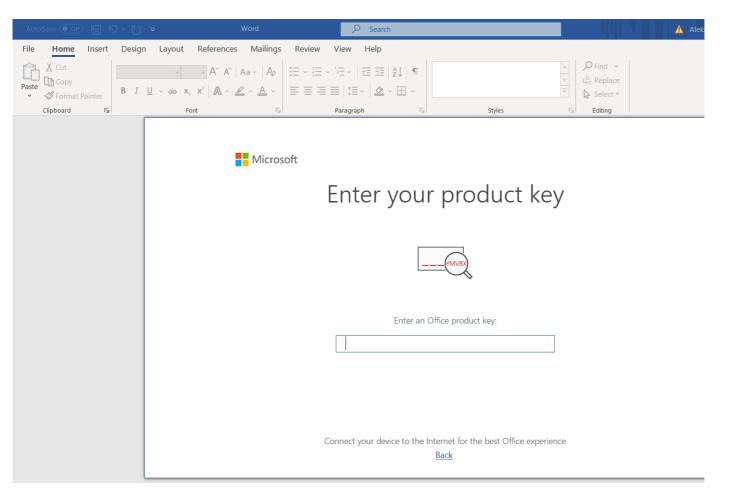
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\lf\52C64B7E\LanguageList Value: en-US\0en\0	2416
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, 70dddf40) Return: 0	2416
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, 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		2416
	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0	
Call WMI API	API Name: WbemServices::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:	2416
Call WIVII AFT	0	2410
Write Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\7x% Value: None	2416
Add File	, , ,	2416
	Path: %APPDATA%Microsoft\Templates\-\\$Normal.dotm Type: VSDT_COM_DOS	
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\RoamingLastSyncTime\Word Value: None	2416
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastWriteTimeWord Value: None	2416
	Key: HKEY CURRENT USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None	2416
Write Registry Key	,	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resillency\StartupItems\% 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% 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\Startup\tems\1\% 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\Current\Version\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\Current\Version\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\Current\Version\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		2416
	API Name: socket Args: (23, 2, 0) Return: c30	
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: N	2416
Write Registry Key	one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Val	2416
	ue: None	
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
	API Name: socket Args: (2, 1, 6) Return: c3c	2416
Call Network API	API Name: bind Args: (c3c, 0.0.0.049167, 128) Return: 0	2416
Call Network API Call Network API		2416
	API Name: ConnectEx Args: (c3c, autodiscover.gmail.com:443, 16, 0, 0, 0, 792bab78) Return: 0	
Call Network API	API Name: ConnectEx Args: (c3c, autodiscover.gmail.com:443, 16, 0, 0, 0, 792bab78) Return: 0 API Name: send Args: (c3c,, 1, 183) Return: 0	2416
Call Network API Call System API Call Network API	API Name: send Args: (c3c,, 1, 183) Return: 0	
Call Network API Call Network API Call System API Call System API	API Name: send Args: (c3c,, 1, 183) Return: 0 API Name: WinHttpCloseHandle Args: (69953950) Return: 1	2416
Call Network API Call System API Call Network API Call System API Call System API Call System API	API Name: send Args: (c3c,, 1, 183) Return: 0 API Name: WinHttpCloseHandle Args: (69953950) Return: 1 API Name: WinHttpCloseHandle Args: (792ba060) Return: 1	2416 2416
Call Network API Call System API Call System API Call System API	API Name: send Args: (c3c,, 1, 183) Return: 0 API Name: WinHttpCloseHandle Args: (69953950) Return: 1	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, 0.0.0.49170, 16) Return: 0	2416
Call System API	API Name: ConnectEx Args: (114, 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, 0.0.0.49172, 128) Return: 0	2416
Call System API	API Name: ConnectEx Args: (110, 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
	API Name: socket Args: (2, 1, 6) Return: f04	2416
Call Network API		2416
Call Network API Call Network API	API Name: bind Args: (f04, 0.0.0.0:49173, 128) Return: 0	
	API Name: bind Args: (104, 0.0.0.0.49173, 128) Return: 0 API Name: ConnectEx Args: (104, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 7906b208) Return: 0	2416
Call Network API		
Call Network API Call System API Call Network API	API Name: ConnectEx Args: (f04, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 7906b208) Return: 0 API Name: send Args: (f04,, 1, 188) Return: 0	2416
Call Network API Call System API Call System API Call System API	API Name: ConnectEx Args: (f04, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 7906b208) Return: 0 API Name: send Args: (f04,, 1, 188) Return: 0 API Name: WinHttpCloseHandle Args: (69954070) Return: 1	2416 2416 2416
Call Network API Call System API Call Network API	API Name: ConnectEx Args: (f04, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 7906b208) Return: 0 API Name: send Args: (f04,, 1, 188) Return: 0	2416 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, 0.0.0.49176, 128) Return: 0	2416
Call System API		2416
	API Name: ConnectEx Args: (f04, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 792bb258) Return: 0	
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, 0.0.0:49178, 16) Return: 0	2416
Call System API	API Name: ConnectEx Args: (e94, estf.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, ctdd.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\nConnection: Keep-Alivel\n Accept: \times "\n'\nUser-Agent: Microsoft-CryptoAPI/6.3\n\nHost: ctldl.windowsupdate.com\n\n\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\Word\Word\Word\Unlicensed Product)	2416
Call System API	API Name: CryptGenKey Args: (7955e5a0, 6610, 1, 70ddedb8) Return: 1	2416
		2416
Call System API	API Name: CryptExportKey Args: (73016740, 73017620, 1, 0, 0, 70ddedb0) Return: 1	
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%\Microsoff\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}.tm	2416
	p) Return: 1	
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
	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 Write Registry Key	·	
Write Registry Key		2416
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None	2416
Write Registry Key Write Registry Key Call Filesystem API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None API Name: RemoveDirectoryW Args: (%TEMP%\[4E8E2B97-D54D-42D5-8581-BD0D039D2C38\\) Return: 1	2416
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2416\0 Value: None	

Decis Flority Kry	2416
	2416
May	2416
Mail Registy Forg May Perf CHIERTY LEER Administration of the Schommer Clear Teacher Chieval And Service Chieval Service C	2416
	2416
Mich Englanty No.	2416
	2416
Mail Registry Name	2416
13	2416
Sa 58075007E1734 Value 0 Sa 58075007E1734 Value 0 Sa 58075007E1734 Value 0 Sa 58075007E1734 Value 0 Sa 58075007E1734 Value 1 Sa 58075007E1734 Va	2416
Add Registry Key	2416
CA-6800CA-680877 Value Port P	2416
Categorian Cat	2416
California Cal	2416
206-80071677011(7) Water None 206-80071677011(7) Water None 206-8007167701(7) Water None 206-800716701(7) Water None 206-8007180684) Water None 206-80071806844 Water None 206-8007180684 Water None 206-	2416
20E-900716F7011Cy1Cy1Aulaur-0	2416
20E-0007/10F7D11C)Categores Value: None Add Registry Key	2416
A0-38C62738C8E4] Value: None Key: HKEY_CURRENT_USERSoftwareMicrosoft/Office16.0/Common/ClientTelemetryRulesMetadatalwinword.exe/ETWMonitor\(Q2FD33DF.F746-4A10-93 \) A0-28C6273BC8E4 Value: 0 A0-28C6273BC8E4 Value: None A0-28C6273	2416
Myite Registry Key Key: HIKEY_CURRENT_USER/Software/Microsoft/Office/16.0/Common/ClientTelemetry/Rules/Metadata/winword.exe/ETVMonitor/Q2FD33DF-F746-A410-93 Acad Registry Key Key: HIKEY_CURRENT_USER/Software/Microsoft/Office/16.0/Common/ClientTelemetry/Rules/Metadata/winword.exe/ULSMonitor/ Value: None Myite Registry Key Key: HIKEY_CURRENT_USER/Software/Microsoft/Office/16.0/Common/ClientTelemetry/Rules/Metadata/winword.exe/ULSMonitor/ULSA/ICategories Value: 6, 10 Add File Path: **XTEMP%/Diagnostics/WINWORD/App_1616237787008562900_A5286CD1-8030-491F-8C28-682FCF23ECFC log Type: VSDT_ASCII ### File Path: **XTEMP%/Diagnostics/WINWORD/App_1616237787008562900_A5286CD1-8030-491F-8C28-682FCF23ECFC log Type: VSDT_ASCII ### File Path: **XTEMP%/Diagnostics/WINWORD/App_1616237787008562900_A5286CD1-8030-491F-8C28-682FCF23ECFC log Type: VSDT_ASCII ### File Path: **XTEMP%/Diagnostics/WINWORD/App_1616237787010322000_A5286CD1-8030-491F-8C28-682FCF23ECFC log Type: VSDT_ASCII ### File ### File Path: **XTEMP%/Diagnostics/WINWORD/App_1616237787010322000_A5286CD1-8030-491F-8C28-682FCF23ECFC log Type: VSDT_ASCII ### File ###	2416
Add Registry Key Reg: HKEY_CURRENT_USERSoftwareMicrosoftOffice\16.0CommonClientTelemetryRulesMetadatalwinword.exeULSMonitor\UserNone Registry Key Reg: HKEY_CURRENT_USERSoftwareMicrosoftOffice\16.0CommonClientTelemetryRulesMetadatalwinword.exeULSMonitor\UserNone Reg: HKEY_CURRENT_USERSoftwareMicrosoftOffice\16.0CommonClientTelemetryRulesMetadatalwinword.exeULSMonitor\UserNone Path: %TEMP%\Diagnostics\Win\WORD\App_1616237787008562900_A5286CD1-8030-491F-8C28-682FCF23ECFC.log Type: VSDT_ASCII Path: %TEMP%\Diagnostics\Win\WORD\App_1616237787008562900_A5286CD1-8030-491F-8C28-682FCF23ECFC.log Type: VSDT_ASCII Path: %TEMP%\Diagnostics\Win\WORD\App_1616237787010322000_A5286CD1-8030-491F-8C28-682FCF23ECFC.log Type: VSDT_EMPTY Write File Path: %TEMP%\Diagnostics\Win\WORD\App_1616237787010322000_A5286CD1-8030-491F-8C28-682FCF23ECFC.log Type: VSDT_EMPTY Write File Path: %TEMP%\Diagnostics\Win\WORD\App_1616237787010322000_A5286CD1-8030-491F-8C28-682FCF23ECFC.log Type: VSDT_EMPTY Write Registry Key Registry Key Registry Key: HKEY_CURRENT_USERSoftware/MicrosoftOffice\16.0CommonLicensing/BootTimeSkuOverride\100c5CCACD-A7AC-4FD3-9F70-945485DE5161\100c3 Registry Key: HKEY_CURRENT_USERSoftware/MicrosoftOffice\16.0CommonLicensing/BootTimeSkuOverride\100c5CCACD-A7AC-4FD3-9F70-945485DE5161\100c3CCACD-A7AC-4FD3-9F70-945485D	2416
Write Registry Key Key: HKEY_CURRENT_USERISoftware\MicrosoftOffice\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ULS\Monitor\ULS\All\Categories\Value: 6, 10 Add File Path: \(\text{TEMP\(\text{N}\)Diagnostics\(\text{WINWORD\(\text{App.}}\) 166237787008562900, \(\text{A5286CD1-8030-491F-8C28-68E2FCF23ECFC.log\) Type: VSDT_ASCII Write File Path: \(\text{TEMP\(\text{M}\)Diagnostics\(\text{WINWORD\(\text{App.}}\) 1616237787008562900, \(\text{A5286CD1-8030-491F-8C28-68E2FCF23ECFC.log\) Type: VSDT_ASCII Add File Path: \(\text{TEMP\(\text{M}\)Diagnostics\(\text{WINWORD\(\text{App.}}\) 1616237787010322000, \(\text{A5286CD1-8030-491F-8C28-68E2FCF23ECFC.log\) Type: VSDT_EMPTY Mrite File Path: \(\text{TEMP\(\text{W}\)Diagnostics\(\text{WINWORD\(\text{App.}}\) 1616237787010322000, \(\text{A5286CD1-8030-491F-8C28-68E2FCF23ECFC.log\) Type: VSDT_EMPTY Add Registry Key Rey: HKEY_CURRENT_USER\(\text{Software\(\text{Microsoft\(\text{Office\)}\) 1600-2000 (\text{A5286CD1-8030-491F-8C28-68E2FCF23ECFC.log\) Type: VSDT_EMPTY Add Registry Key Rey: HKEY_CURRENT_USER\(\text{Software\(\text{Microsoft\(\text{Office\)}\) 1600-2000 (\text{Microsoft\(\text{Office\)}\) 1600-2000 (\text{Microsoft\(\text{Office\)}\) 1600-2000 (Microsoft\(\text{D4786000000000000000000000000000000000000	2416
10 Path: %TEMP%\Diagnostics\WINWORD\App_1616237787008562900_A5286CD1-8030-491F-8C28-682FCF23ECFC.log Type: VSDT_ASCII Write File	2416
Write File Path: %TEMP%\Diagnostics\WINWORD\App_1616237787008562900_A5286CD1-8030-491F-8C28-6B2FCF23ECFC.log Type: VSDT_ASCII Add File Path: %TEMP%\Diagnostics\WINWORD\App_1616237787010322000_A5286CD1-8030-491F-8C28-6B2FCF23ECFC.log Type: VSDT_EMPTY Write File Path: %TEMP%\Diagnostics\WINWORD\App_1616237787010322000_A5286CD1-8030-491F-8C28-6B2FCF23ECFC.log Type: VSDT_EMPTY Add Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Llcensing\Boot\TimeSkuOverride\Value: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Llcensing\Boot\TimeSkuOverride\\Dicord\Di	2416
Add File Path: %TEMP%/Diagnostics/WINWORD/App_161623778701032200_A5286CD1-8030-491F-8C28-6B2FCF23ECFC.log Type: VSDT_EMPTY Write File Path: %TEMP%/Diagnostics/WINWORD/App_161623778701032200_A5286CD1-8030-491F-8C28-6B2FCF23ECFC.log Type: VSDT_EMPTY Add Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Licensing\BootTimeSku\Override\Value: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Licensing\BootTimeSku\Override\Value: None Write Registry Key key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Licensing\BootTimeSku\Override\\DC5CCACD-A7AC-4FD3-9F70-9454B5DE5161\) Va lue: (D7279DD0-E175-49FE-A623-8FC2FC00AFC4\) Call System API API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 Call Internet Helper API API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, ., ., 3, 0, 1770995072) Return: cc00008 Call Internet Helper API API Name: socket Args: (cc0004, self.events.data.microsoft.com, 443, ., ., 3, 0, 1770995072) Return: cc0000 Call Network API API Name: socket Args: (2, 1, 6) Return: 958 Call Network API API Name: Socket Args: (958, 0.0.0.49181, 16) Return: 0 Call System API API Name: Send Args: (958, self.events.data.microsoft.com:443, 16, 0, 0, 0, 73018b98) Return: 0 Call Network API API Name: Send Args: (958, self.events.data.microsoft.com:443, 16, 0, 0, 0, 73018b98) Return: 0 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-shm) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-shm) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-shm) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%TEMP%\(A5286CD1-8030-491F-8C28-6B2FCF23ECFC) - OProcSessId.dat) Return: 1	2416
Write File Path: %TEMP%(Diagnostics\WINWORD\App_161623778701032200_A5286CD1-8030-491F-8C28-6B2FCF23ECFC.log Type: VSDT_EMPTY Add Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Licensing\Boot\TimeSkuOverride\Value: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Licensing\Boot\TimeSkuOverride\\Delta\Universide\Del	2416
Add Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Licensing\Boot\TimeSkuOverride\\Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Licensing\Boot\TimeSkuOverride\\DCSCCACD-A7AC-4FD3-9F70-9454B5DE5161) Value: (D7279DDD-E175-49FE-A623-8FC2FC00AFC4) Call System API API Name: DisoQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 Call Internet Helper API API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 1770995072) Return: cc0008 Call Internet Helper API API Name: Socket Args: (2, 1, 6) Return: 958 Call Network API API Name: Socket Args: (958, 0.0.0.49181, 16) Return: 0 Call System API API Name: ConnectEx Args: (958, self.events.data.microsoft.com:443, 16, 0, 0, 0, 73018b98) Return: 0 Call Network API API Name: Send Args: (958,, 1, 191) Return: 0 Call Filesystem API API Name: DeleteFileW Args: (\(\frac{1}{2}\) MLOCALAPPDATA\%Microsoft\Office\OTele\winword.exe.db-shm\) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (\(\frac{1}{2}\) MLOCALAPPDATA\%Microsoft\Office\OTele\winword.exe.db-shm\) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (\(\frac{1}{2}\) MLOCALAPPDATA\%Microsoft\Office\OTele\winword.exe.db-shm\) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (\(\frac{1}{2}\) MLOCALAPPDATA\%Microsoft\Office\OTele\winword.exe.db-shm\) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (\(\frac{1}{2}\) MLOCALAPPDATA\%Microsoft\Office\OTele\winword.exe.db-shm\) Return: 1	2416
Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Licensing\BootTimeSkuOverride\[DC5CCACD-A7AC-4FD3-9F70-9454B5DE5161\] Value: \(\text{D7279DD0-E175-49FE-A623-8FC2FC00AFC4\}\) Call System API API Name: DiscoueryEx Args: \(\text{cents.data.microsoft.com.} 1, 50020000\) Return: 9003 Call Internet Helper API API Name: InternetConnectA Args: \(\text{ce0004}, \text{self.events.data.microsoft.com.} 443, , , 3, 0, 1770995072\) Return: cc0008 Call Network API API Name: socket Args: \(\text{ce0008}, \text{POST}, \text{OneCollector/1.0/, , 2061562408, -2067004672, 1770995072\) Return: cc000c Call Network API API Name: socket Args: \(\text{958}, 0.0.0.049181, 16\) Return: 0 Call System API API Name: ConnectEx Args: \(\text{958}, 0.0.0.049181, 16\) Return: 0 Call Network API API Name: send Args: \(\text{958},, 1, 191\) Return: 0 Call Filesystem API API Name: DeleteFileW Args: \(VACALAPPDATA\%Microsoft\Office\OTele\winword.exe.db-shm\) Return: 1 Call Filesystem API API Name: DeleteFileW Args: \(\text{VACALAPPDATA\%Microsoft\Office\OTele\winword.exe.db-shm\) Return: 1 Call Filesystem API API Name: DeleteFileW Args: \(\text{VACEALAPPDATA\%Microsoft\Office\OTele\winword.exe.db-shd\) Return: 1 Call Filesystem API API Name: DeleteFileW Args: \(\text{VACEALAPPDATA\%Microsoft\Office\OTele\winword.exe.db-shd\) Return: 1 Call Filesystem API API Name: DeleteFileW Args: \(\text{VACEALAPPDATA\%Microsoft\Office\OTele\winword.exe.db-shd\) Return: 1	2416
Liue: {D7279DD0-E175-49FE-A628-BFC2FC00AFC4} Call System API API Name: DnsQueryEx Args: (self. events.data.microsoft.com, 1, 50020000) Return: 9003 Call Internet Helper API API Name: InternetConnectA Args: (cc0004, self. events.data.microsoft.com, 443, . , 3, 0, 1770995072) Return: cc0008 Call Internet Helper API API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, . , 2061562408, -2067004672, 1770995072) Return: cc000c Call Network API API Name: socket Args: (2, 1, 6) Return: 958 Call System API API Name: SonnectEx Args: (958, 0.0.0.49181, 16) Return: 0 Call Network API API Name: ConnectEx Args: (958, self. events.data.microsoft.com:443, 16, 0, 0, 0, 73018b98) Return: 0 Call Network API API Name: send Args: (958,, 1, 191) Return: 0 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-shm) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-smal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-smal) Return: 1	2416
Call Internet Helper API API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 1770995072) Return: cc0008 Call Internet Helper API API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2061562408, -2067004672, 1770995072) Return: cc000c Call Network API API Name: socket Args: (2, 1, 6) Return: 958 Call Network API API Name: ConnectEx Args: (958, 0.0.0.0:49181, 16) Return: 0 Call System API API Name: ConnectEx Args: (958, self.events.data.microsoft.com:443, 16, 0, 0, 0, 73018b98) Return: 0 Call Network API API Name: send Args: (958,, 1, 191) Return: 0 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoft!Office\OTele\winword.exe.db-shn) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoft!Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoft!Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoft!Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoft!Office\OTele\winword.exe.db-wal) Return: 1	2416
Call Internet Helper API API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 1770995072) Return: cc0008 Call Internet Helper API API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2061562408, -2067004672, 1770995072) Return: cc000c Call Network API API Name: socket Args: (2, 1, 6) Return: 958 Call Network API API Name: DeleteFileW Args: (958, 0.0.0.0:49181, 16) Return: 0 Call System API API Name: ConnectEx Args: (958, self.events.data.microsoft.com:443, 16, 0, 0, 0, 73018b98) Return: 0 Call Network API API Name: send Args: (958,, 1, 191) Return: 0 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoft!Office\OTele\winword.exe.db-shm) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoft!Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoft!Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoft!Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoft!Office\OTele\winword.exe.db-wal) Return: 1	2416
Call Internet Helper API API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , 2061562408, -2067004672, 1770995072) Return: cc000c Call Network API API Name: bind Args: (958, 0.0.0.049181, 16) Return: 0 Call System API API Name: ConnectEx Args: (958, self.events.data.microsoft.com:443, 16, 0, 0, 0, 73018b98) Return: 0 Call Network API API Name: send Args: (958,, 1, 191) Return: 0 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%IMicrosoft!Office\OTele\winword.exe.db-shm) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft!Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft!Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft!Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft!Office\OTele\winword.exe.db-wal) Return: 1	2416
Call Network API API Name: socket Args: (2, 1, 6) Return: 958 Call Network API API Name: beleteFileW Args: (958, 0.0.0.49181, 16) Return: 0 Call System API API Name: ConnectEx Args: (958, self-events.data.microsoft.com:443, 16, 0, 0, 0, 73018b98) Return: 0 Call Network API API Name: send Args: (958, s., 1, 191) Return: 0 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-shm) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%TEMPS\(\)\(A5286CD1-8030-491F-8C28-6B2FCF23ECFC) - OProcSessId.dat) Return: 1	2416
Call Network API API Name: bind Args: (958, 0.0.0.49181, 16) Return: 0 Call System API API Name: ConnectEx Args: (958, self.events.data.microsoft.com:443, 16, 0, 0, 0, 73018b98) Return: 0 Call Network API API Name: send Args: (958,, 1, 191) Return: 0 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-shm) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%TEMPS\(\)\(A5286CD1-8030-491F-8C28-6B2FCF23ECFC) - OProcSessId.dat) Return: 1	2416
Call System API API Name: ConnectEx Args: (958, self.events.data.microsoft.com:443, 16, 0, 0, 0, 73018b98) Return: 0 Call Network API API Name: send Args: (958,, 1, 191) Return: 0 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-shm) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%TEMP%\(A5286CD1-8030-491F-8C28-6B2FCF23ECFC) - OProcSessId.dat) Return: 1	2416
Call Network API API Name: send Args: (958,, 1, 191) Return: 0 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-shm) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%TEMP%\(A5286CD1-8030-491F-8C28-6B2FCF23ECFC) - OProcSessId.dat) Return: 1	2416
Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-shm) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%TEMP%\(A5286CD1-8030-491F-8C28-6B2FCF23ECFC) - OProcSessId.dat) Return: 1	2416
Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\OTele\winword.exe.db-wal) Return: 1 Call Filesystem API API Name: DeleteFileW Args: (%TEMP%\(A5286CD1-8030-491F-8C28-6B2FCF23ECFC) - OProcSessId.dat) Return: 1	2416
Call Filesystem API API Name: DeleteFileW Args: (%TEMP%\(A5286CD1-8030-491F-8C28-6B2FCF23ECFC) - OProcSessId.dat) Return: 1	2416
	2416
	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

