Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-02-22 11:51:14
Submitter	Manual Submission
Type	MS OLE document

Analysis Overview

Overall risk level	High risk	The object exhibited highly suspicious characteristics that are commonly associated with malware.	
Detections	TROJ_FRS.0NA103BC21		
Exploited vulnerabilities	-		
Analyzed objects	MS OLE document	1 - TELEGRAPHIC TRANSFER.xlsx	3E9C74BF533C67AF4DCD3E8C63FC03982CB9E3C0
	Office Excel 2007 spreadsheet	1.1 - NONAMEFL	3B134E01EFAF603E47362FBA1C35E6D3D63F01F2
	Office Word 2007 document	1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm	5D9887AF2E228247570142E1CDB42BE7A8DCEBF1

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

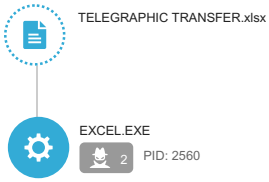
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.0NA103BC21
Exploited vulnerabilities	-
Network connection	No network

Object 1 - TELEGRAPHIC TRANSFER.xlsx (MS OLE document)

File name	TELEGRAPHIC TRANSFER.xlsx
File type	MS OLE document
SHA-1	3E9C74BF533C67AF4DCD3E8C63FC03982CB9E3C0
SHA-256	95736440E01059DE4F8E0258F3CE84F7D450BC5C96432D8DA5F82162C3E96371
MD5	C4D4887B6F12121169ABBF810576B286
Size	2485248 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.0NA103BC21
Exploited vulnerabilities	-
Threat Characteristics	Hijack, redirection, or data theft (2) Malformed, defective, or with known malware traits (1) Suspicious network or messaging activity (15)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Windows Management Instrumentation	Characteristics: 1, 2
Discovery	System Information Discovery	Characteristics: 1, 2

Notable Threat Characteristics

Hijack, redirection, or data theft (2)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information		Process ID: 2560 Info: Obtains Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%' from API result
Executes commands or uses API to obtain system information		Process ID: 2560 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.0NA103BC21 Engine Version: 12.500.1008 Malware Pattern Version: 16.551.92

Suspicious network or messaging activity (15)

Characteristic	Significance	Details
Listens on port	■□□	0.0.0.0:49181
Listens on port	■□□	0.0.0.0:49180
Listens on port	■□□	0.0.0.0:49179
Listens on port	■□□	0.0.0.0:49178
Listens on port	■□□	0.0.0.0:49177
Listens on port	■□□	0.0.0.0:49176
Listens on port	■□□	0.0.0.0:49175
Listens on port	■□□	0.0.0.0:49174
Listens on port	■□□	0.0.0.0:49173
Listens on port	■□□	0.0.0.0:49172
Listens on port	■□□	0.0.0.0:49171
Listens on port	■□□	0.0.0.0:49170
Listens on port	■□□	0.0.0.0:49169
Listens on port	■□□	0.0.0.0:49168
Listens on port	■□□	127.0.0.1:49470

Network Destinations

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

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

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
excel.exe.db-shm	No risk	-	-	-	32768	0C8F8CB3DF2C60487F1ACF6B91970B21398C284D
excel.exe.db-wal	No risk	-	-	-	4152	812D6E59F1D3F3C43330CA45557F4821060C1A1E
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	302	F5D7383EFFD6A0E8F382C86278402FB04566509C
App_1613987768419572400_7982ADFC-4416-4335-8524-FB4800B0D1F0.log	No risk	-	-	-	20971520	9674344C90C2F0646F0B78026E127C9B86E3AD77
App_1613987768416669600_7982ADFC-4416-4335-8524-FB4800B0D1F0.log	No risk	-	-	-	20971520	A781B537854FA21092F36265BFF9AE2E9DD0AEFD
{7982ADFC-4416-4335-8524-FB4800B0D1F0} - OProcSessId.dat	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	3E9C74BF533C67AF4DCD3E8C63FC03982CB9E3C0	High

Analysis

Event Type	Details	Parent PID	PID

Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.0NA103BC21 Engine Version: 12.500.1008 Malware Pattern Version: 16.551.92		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ClientTelemetry\Sampling\1 Value: None		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2560\ Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2560\0 Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\mc& Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ImmersiveWorkbookDirtySentinel Value: 0		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ExcelWorkbookOpenedCount Value: 0		2560
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\Diagnostics\EXCEL\App_1600985250979406400_37DFED58-65EC-4733-9903-AF526D736AF9.log) Return: 1		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\EXCEL\2704\0 Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\EXCEL\2704\ Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2560\0 Value: None		2560
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, e592f5b0) Return: 0		2560
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, e592f5b0) Return: 0		2560
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, e592f4f0) Return: 0		2560
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2560 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		2560
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, e592f4f0) Return: 0		2560
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2560 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		2560
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, e592f4f0) Return: 0		2560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\f\52C64B7E\LanguageList Value: en-US\0en\0		2560
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, e592e300) Return: 0		2560
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, e592e300) Return: 0		2560
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, e592e240) Return: 0		2560
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0		2560
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, e592e240) Return: 0		2560
Call WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0		2560
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, e592e240) Return: 0		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastSyncTimeExcel Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastWriteTimeExcel Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\mc& Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: 9a0		2560
Call Network API	API Name: bind Args: (9a0, 127.0.0.1:49470, 128) Return: 0		2560
Detection	Threat Characteristic: Listens on port 127.0.0.1:49470		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2560\0 Value: None		2560
Call Network API	API Name: socket Args: (23, 1, 6) Return: ae4		2560
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (e5c7e1b0, 0, 0, 0) Return: 1		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2560
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0004		2560
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (e5c7e050, 0, 0, 0) Return: 1		2560
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (e5c7e020, 0, 0, 0) Return: 1		2560
Call Network API	API Name: socket Args: (2, 1, 0) Return: a40		2560
Call Network API	API Name: socket Args: (23, 1, 6) Return: b5c		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\SessionId Value: None		2560
Call System API	API Name: WinHttpCloseHandle Args: (efb284d0) Return: 1		2560
Call Network API	API Name: socket Args: (23, 1, 6) Return: bc8		2560
Call System API	API Name: WinHttpCloseHandle Args: (efb29850) Return: 1		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: c38		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: c38		2560
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87		2560
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003		2560

Call Network API	API Name: socket Args: (23, 2, 0) Return: c38		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: c38		2560
Call Network API	API Name: bind Args: (c38, 0.0.0.0:49168, 128) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49168		
Call System API	API Name: ConnectEx Args: (c38, gmail.com:443, 16, 0, 0, 0, efeb2ff8) Return: 0		2560
Call Network API	API Name: send Args: (c38, ..., 1, 170) Return: 0		2560
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2560
Call System API	API Name: WinHttpCloseHandle Args: (dd642800) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (efeaffc0) Return: 1		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: e50		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: e50		2560
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1, 40006000) Return: 87		2560
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1c, 40026000) Return: 9003		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: c44		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: c44		2560
Call Network API	API Name: bind Args: (c44, 0.0.0.0:49169, 128) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49169		
Call System API	API Name: ConnectEx Args: (c44, autodiscover.gmail.com:443, 16, 0, 0, 0, efeafe78) Return: 0		2560
Call Network API	API Name: send Args: (c44, ..., 1, 183) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (dd63f620) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (efeb2bc0) Return: 1		2560
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2560
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -361728784) Return: cc0008		2560
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -275057096, -2067004672, -361728784) Return: cc000c		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: e6c		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: e6c		2560
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87		2560
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: e70		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: e70		2560
Call Network API	API Name: bind Args: (e70, 0.0.0.0:49170, 16) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49170		
Call System API	API Name: ConnectEx Args: (e70, self.events.data.microsoft.com:443, 16, 0, 0, 0, ea3c9158) Return: 0		2560
Call Network API	API Name: send Args: (e70, ..., 1, 191) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (efb29100) Return: 1		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: ee4		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: ee4		2560
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2560
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: ef0		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: ef0		2560
Call Network API	API Name: bind Args: (ef0, 0.0.0.0:49171, 128) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49171		
Call System API	API Name: ConnectEx Args: (ef0, ctldl.windowsupdate.com:80, 16, 0, 0, 0, efc8fac8) Return: 0		2560
Call Network API	API Name: send Args: (ef0, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?6a29eacfd4158db9 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		2560
Call System API	API Name: WinHttpCloseHandle Args: (dd63f9b0) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (ea68b0e0) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (e6574e50) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (efb284d0) Return: 1		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: ee0		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: ee0		2560
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2560
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: ebc		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: ebc		2560
Call Network API	API Name: bind Args: (ebc, 0.0.0.0:49172, 128) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49172		
Call System API	API Name: ConnectEx Args: (ebc, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, e65eb618) Return: 0		2560
Call Network API	API Name: send Args: (ebc, ..., 1, 188) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (dd63f620) Return: 1		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: ebc		2560
Call Network API	API Name: bind Args: (ebc, 0.0.0.0:49173, 128) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49173		
Call System API	API Name: ConnectEx Args: (ebc, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, e65ed038) Return: 0		2560
Call Network API	API Name: send Args: (ebc, ..., 1, 188) Return: 0		2560

Call System API	API Name: WinHttpCloseHandle Args: (dd63f620) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (e65eb080) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (e65eaf20) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (efb27d80) Return: 1		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: ec8		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: ec8		2560
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2560
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: ee0		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: ee0		2560
Call Network API	API Name: bind Args: (ee0, 0.0.0.0:49174, 128) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49174		
Call System API	API Name: ConnectEx Args: (ee0, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, e65ec3d8) Return: 0		2560
Call Network API	API Name: send Args: (ee0, ..., 1, 188) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (dd63f620) Return: 1		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: ed4		2560
Call Network API	API Name: bind Args: (ed4, 0.0.0.0:49175, 128) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49175		
Call System API	API Name: ConnectEx Args: (ed4, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, e65eaf38) Return: 0		2560
Call Network API	API Name: send Args: (ed4, ..., 1, 188) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (dd63f620) Return: 1		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: ed4		2560
Call Network API	API Name: bind Args: (ed4, 0.0.0.0:49176, 128) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49176		
Call System API	API Name: ConnectEx Args: (ed4, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, e65eb618) Return: 0		2560
Call Network API	API Name: send Args: (ed4, ..., 1, 188) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (dd63f620) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (e65e9be0) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (e65e9a80) Return: 1		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: ed4		2560
Call Network API	API Name: bind Args: (ed4, 0.0.0.0:49177, 128) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call System API	API Name: ConnectEx Args: (ed4, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, e65ebcf8) Return: 0		2560
Call Network API	API Name: send Args: (ed4, ..., 1, 188) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (dd63f620) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (e65e9d40) Return: 1		2560
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2560
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -361712224) Return: cc0008		2560
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -275057096, -2067004672, -361712224) Return: cc000c		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: ebc		2560
Call Network API	API Name: bind Args: (ebc, 0.0.0.0:49178, 16) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49178		
Call System API	API Name: ConnectEx Args: (ebc, self.events.data.microsoft.com:443, 16, 0, 0, 0, ea3c9e78) Return: 0		2560
Call Network API	API Name: send Args: (ebc, ..., 1, 191) Return: 0		2560
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2560
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -361710016) Return: cc0008		2560
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -275057096, -2067004672, -361710016) Return: cc000c		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: 728		2560
Call Network API	API Name: bind Args: (728, 0.0.0.0:49179, 16) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49179		
Call System API	API Name: ConnectEx Args: (728, self.events.data.microsoft.com:443, 16, 0, 0, 0, ea3ccdb8) Return: 0		2560
Call Network API	API Name: send Args: (728, ..., 1, 191) Return: 0		2560
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2560
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -361707808) Return: cc0008		2560
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -275057096, -2067004672, -361707808) Return: cc000c		2560
Call System API	API Name: WinHttpCloseHandle Args: (efb28740) Return: 1		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: 728		2560
Call Network API	API Name: bind Args: (728, 0.0.0.0:49180, 16) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49180		
Call System API	API Name: ConnectEx Args: (728, self.events.data.microsoft.com:443, 16, 0, 0, 0, ea3c3d58) Return: 0		2560
Call Network API	API Name: send Args: (728, ..., 1, 191) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (efb29850) Return: 1		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: ed4		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: ed4		2560
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2560
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2560

Call Network API	API Name: socket Args: (23, 2, 0) Return: ec8		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: ec8		2560
Call Network API	API Name: bind Args: (ec8, 0.0.0.0:49181, 128) Return: 0		2560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49181		
Call System API	API Name: ConnectEx Args: (ec8, ctldl.windowsupdate.com:80, 16, 0, 0, 0, e65c3478) Return: 0		2560
Call Network API	API Name: send Args: (ec8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?3fffaea1a1374377 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		2560
Call System API	API Name: WinHttpCloseHandle Args: (dd63f9b0) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (ea68a5e0) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (e6574690) Return: 1		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security\Trusted Documents\ Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 19a7555		2560

Screenshot

Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	3B134E01EFAF603E47362FBA1C35E6D3D63F01F2
SHA-256	9708758A46BFA696D7C10D4446A57405C4E041D3BE09DD94A03511AE9E9553C0
MD5	89DAB94FDF533F66470AE326AF554154
Size	2461856 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

Network Destinations

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

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

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
L1HKFC8L23CTV9YZSOH7.temp	No risk	-	-	-	7682	490ABC04D54945FD432844E28BA8453CDCDD6131
excel.exe.db-shm	No risk	-	-	-	32768	ED6974544817FD3DA53CB30631049327B330464E
excel.exe.db-wal	No risk	-	-	-	4152	9CB25A6D042044135142BB96A9B1F62C390C07E0
b8ab77100df80ab2.customDestinations-ms	No risk	-	-	-	7682	490ABC04D54945FD432844E28BA8453CDCDD6131
~$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACBC431721
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	302	AD4406E2D8C67F8AB6654EE69B6BAC4CF859C1C5
40056F05.emf	No risk	-	-	-	653280	F14C56A7AD5EB26E616BC6041EC67F0D827564B4
App_161398750560625910 0_F732E67-19B2-4714-A063-39622B960F53.log	No risk	-	-	-	16722	74741B572CEF0DA79073F7162BF8E024DCAFF8A6
41FFA142.png	No risk	-	-	-	22200	A9FFED8E6115507A568EE4E9909A94412270563B
App_161398750560894590 0_F732E67-19B2-4714-A063-39622B960F53.log	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

Analysis

Event Type	Details	Parent PID	PID
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ClientTelemetry\Sampling\1 Value: None		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2560\ Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2560\0 Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\o ' Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ImmersiveWorkbookDirtySentinel Value: 0		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ExcelWorkbookOpenedCount Value: 0		2560
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\Diagnostics\EXCEL\App_1600985250979406400_37DFED58-65EC-4733-9903-AF526D736AF9.log) Return: 1		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\EXCEL\2704\0 Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\EXCEL\2704\ Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2560\0 Value: None		2560
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, 8daaf5d0) Return: 0		2560
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 8daaf5d0) Return: 0		2560
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 8daaf510) Return: 0		2560
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0		2560
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, 8daaf510) Return: 0		2560
Call WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0		2560
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, 8daaf510) Return: 0		2560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\f\52C64B7E\LanguageList Value: en-US\0en\0		2560
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, 8daae320) Return: 0		2560
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 8daae320) Return: 0		2560
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 8daae260) Return: 0		2560
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0		2560
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, 8daae260) Return: 0		2560
Call WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0		2560
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, 8daae260) Return: 0		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastSyncTimeExcel Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastWriteTimeExcel Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\o ' Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\6/' Value: None		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D0737\ Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D0737\1D0737 Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ExcelWorkbookOpenedCount Value: 1		2560

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D0737\1D0737 Value: None		2560
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		2560
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2560) Return: 1		2560
Call Network API	API Name: socket Args: (23, 1, 6) Return: a14		2560
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (8dbae120, 0, 0, 0) Return: 1		2560
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0004		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2560
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (8dbadfc0, 0, 0, 0) Return: 1		2560
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (8dbadf90, 0, 0, 0) Return: 1		2560
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\Program) Return: 1		2560
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2560) Return: 1		2560
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2560
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -1901609840) Return: cc0008		2560
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -1767182744, -2067004672, -1901609840) Return: cc000c		2560
Call System API	API Name: WinHttpCloseHandle Args: (8eb18900) Return: 1		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: aec		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: aec		2560
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87		2560
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: b0c		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: b0c		2560
Call Network API	API Name: bind Args: (b0c, 0.0.0.0:49170, 16) Return: 0		2560
Call System API	API Name: ConnectEx Args: (b0c, self.events.data.microsoft.com:443, 16, 0, 0, 0, 921f3728) Return: 0		2560
Call Network API	API Name: send Args: (b0c, ..., 1, 191) Return: 0		2560
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2560
Call System API	API Name: WinHttpCloseHandle Args: (8e85a590) Return: 1		2560
Call Network API	API Name: socket Args: (23, 1, 6) Return: d74		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: dd0		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: dd0		2560
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2560
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: dd8		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: dd8		2560
Call Network API	API Name: bind Args: (dd8, 0.0.0.0:49171, 128) Return: 0		2560
Call System API	API Name: ConnectEx Args: (dd8, ctldl.windowsupdate.com:80, 16, 0, 0, 0, 8e8b3018) Return: 0		2560
Call Network API	API Name: send Args: (dd8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?85d33f96a2e815cd 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		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: f24		2560
Call Network API	API Name: bind Args: (f24, 127.0.0.1:60707, 128) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (8e8cd370) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (8e8b0c40) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (92214c00) Return: 1		2560
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII		2560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\v1.7\hostproperties.json Type: VSDT_ASCII		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D0737\1D0737 Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D0737\ Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\6/' Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D2FED\ Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D2FED\1D2FED Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2560\0 Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2560\0 Value: None		2560
Call Network API	API Name: socket Args: (23, 1, 6) Return: fc4		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: 1038		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: 1038		2560
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2560
Call System API	API Name: WinHttpCloseHandle Args: (8e85b430) Return: 1		2560
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: 102c		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: 102c		2560
Call Network API	API Name: bind Args: (102c, 0.0.0.0:49172, 128) Return: 0		2560

Call System API	API Name: ConnectEx Args: (102c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 9606d0a8) Return: 0		2560
Call Network API	API Name: send Args: (102c, ..., 1, 188) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (8ea3fba0) Return: 1		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: 102c		2560
Call Network API	API Name: bind Args: (102c, 0.0.0.0:49173, 128) Return: 0		2560
Call System API	API Name: ConnectEx Args: (102c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 9606c2e8) Return: 0		2560
Call Network API	API Name: send Args: (102c, ..., 1, 188) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (8ea3f0f0) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (9606dfb0) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (9606a490) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (8e85b430) Return: 1		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: 103c		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: 103c		2560
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2560
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: 103c		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: 103c		2560
Call Network API	API Name: bind Args: (103c, 0.0.0.0:49174, 128) Return: 0		2560
Call System API	API Name: ConnectEx Args: (103c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 9606dfc8) Return: 0		2560
Call Network API	API Name: send Args: (103c, ..., 1, 188) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (8ea422d0) Return: 1		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: 103c		2560
Call Network API	API Name: bind Args: (103c, 0.0.0.0:49175, 128) Return: 0		2560
Call System API	API Name: ConnectEx Args: (103c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 9606c188) Return: 0		2560
Call Network API	API Name: send Args: (103c, ..., 1, 188) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (8ea422d0) Return: 1		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: 103c		2560
Call Network API	API Name: bind Args: (103c, 0.0.0.0:49176, 128) Return: 0		2560
Call System API	API Name: ConnectEx Args: (103c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 9606c448) Return: 0		2560
Call Network API	API Name: send Args: (103c, ..., 1, 188) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (8ea3f810) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (9606c2d0) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (9606ba90) Return: 1		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: 103c		2560
Call Network API	API Name: bind Args: (103c, 0.0.0.0:49177, 128) Return: 0		2560
Call System API	API Name: ConnectEx Args: (103c, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 9606e128) Return: 0		2560
Call Network API	API Name: send Args: (103c, ..., 1, 188) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (8ea3f0f0) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (9606b7d0) Return: 1		2560
Call Network API	API Name: socket Args: (2, 1, 0) Return: 102c		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\SessionId Value: None		2560
Call System API	API Name: WinHttpCloseHandle Args: (8e85b430) Return: 1		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: 1078		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: 1078		2560
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87		2560
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: dd4		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: dd4		2560
Call Network API	API Name: bind Args: (dd4, 0.0.0.0:49178, 128) Return: 0		2560
Call System API	API Name: ConnectEx Args: (dd4, gmail.com:443, 16, 0, 0, 0, 9606cc88) Return: 0		2560
Call Network API	API Name: send Args: (dd4, ..., 1, 170) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (8ea3fba0) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (9606c6f0) Return: 1		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: 107c		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: 107c		2560
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1, 40006000) Return: 87		2560
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1c, 40026000) Return: 9003		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: 107c		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: 107c		2560
Call Network API	API Name: bind Args: (107c, 0.0.0.0:49179, 128) Return: 0		2560
Call System API	API Name: ConnectEx Args: (107c, autodiscover.gmail.com:443, 16, 0, 0, 0, 9606a4a8) Return: 0		2560
Call Network API	API Name: send Args: (107c, ..., 1, 183) Return: 0		2560
Call System API	API Name: WinHttpCloseHandle Args: (8ea422d0) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (9606aa10) Return: 1		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\File MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\File MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\User MRU\LiveId_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C495056D56BADD0D4\File MRU\ Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\User MRU\LiveId_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C495056D56BADD0D4\File MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\User MRU\LiveId_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C495056D56BADD0D4\File MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Place MRU\ Value: None		2560

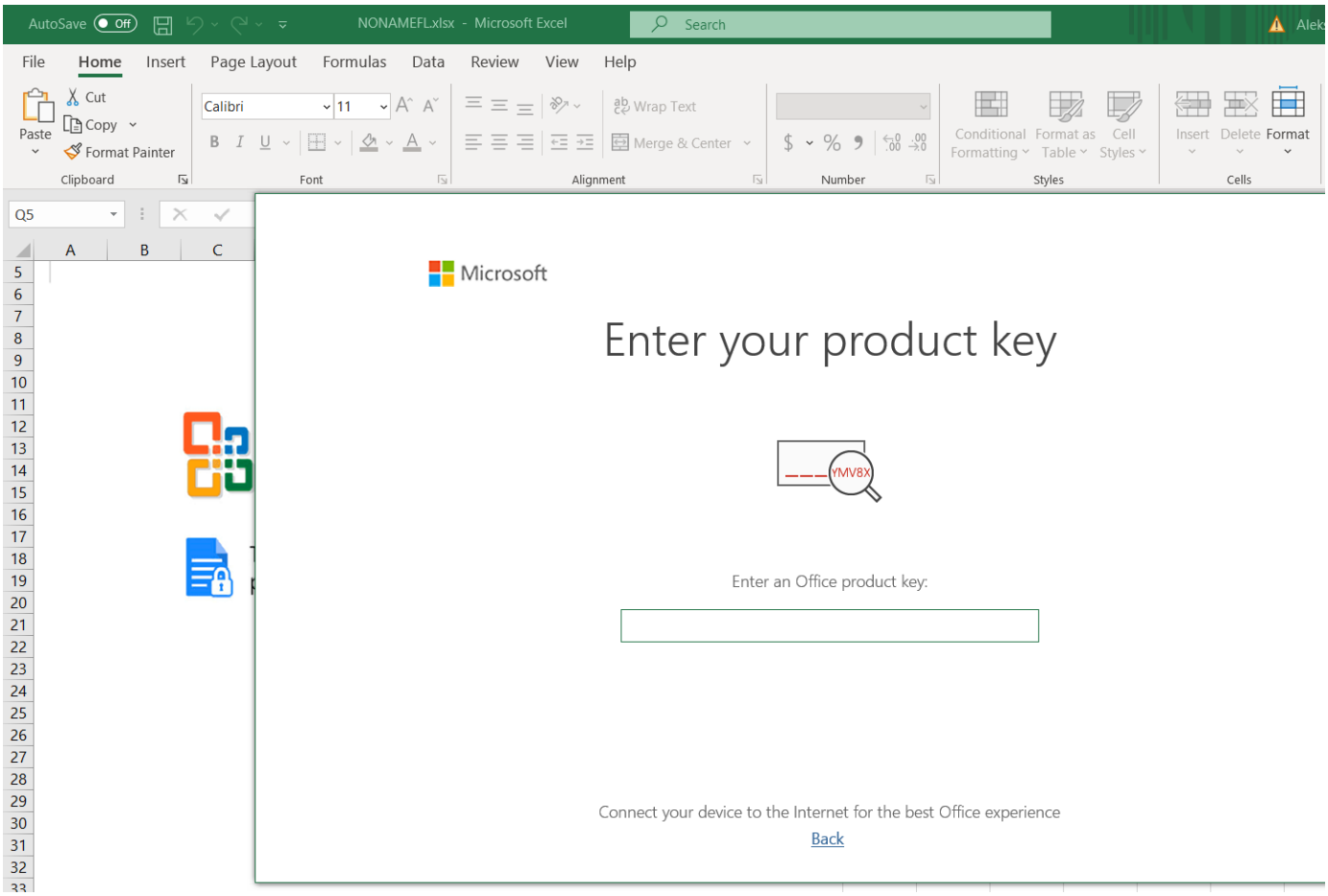
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Place MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Place MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xls\OpenWithProgids\Excel.Sheet.8 Value: None		2560
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, fb531318, -1, 8f51d3c0, 8f51d3c8, 0) Return: 0		2560
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\L1HKFC8L23CTV9YZSOH7.temp Type: VSDT_COM_DOS		2560
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\L1HKFC8L23CTV9YZSOH7.temp Type: VSDT_COM_DOS		2560
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\b8ab77100df80ab2.customDestinations-ms Type: VSDT_COM_DOS		2560
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{9B92EB61-CBC1-11D3-8C2D-00A0CC37B591}\1.2\(Default) Value: Microsoft Smart Tags 2.0 Type Library		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-A27D-11D3-BD33-D80C46980A07}\ Value: None		2560
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		2560
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		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-A27D-11D3-BD33-D80C46980A07}\ProxyStubClsid32\ Value: None		2560
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		2560
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		2560
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		2560
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		2560
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		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3C6C0440-A27D-11D3-BD33-D80C46980A07}\TypeLib\Version Value: 1.2		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\(Default) Value: None		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\ProxyStubClsid32\ Value: None		2560
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		2560
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		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B735-11D3-B2CF-00500489D6A3}\TypeLib\ Value: None		2560
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		2560
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		2560
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		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\(Default) Value: None		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\ProxyStubClsid32\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\ProxyStubClsid32\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\ProxyStubClsid32\(Default) Value: None		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\TypeLib\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\TypeLib\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\TypeLib\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{54F37842-CDD7-11D3-B2D4-00500489D6A3}\TypeLib\Version Value: 1.2		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\ Value: None		2560
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		2560
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		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\ProxyStubClsid32\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\ProxyStubClsid32\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\ProxyStubClsid32\(Default) Value: None		2560

Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\TypeLib\ Value: None		2560
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		2560
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		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3B744D8F-B8A5-11D3-B2CF-00500489D6A3}\TypeLib\Version Value: 1.2		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\(Default) Value: None		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\ProxyStubClsid32\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\ProxyStubClsid32\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\ProxyStubClsid32\(Default) Value: None		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\TypeLib\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\TypeLib\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4C62D17-6162-41DE-BE24-5B1D3F529CC3}\TypeLib\(Default) Value: None		2560
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		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{347958C0-E86F-4865-97C8-BED31E4C28E0}\ Value: None		2560
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		2560
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		2560
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		2560
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		2560
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		2560
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		2560
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		2560
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		2560
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		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A4}\ Value: None		2560
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		2560
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		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A4}\ProxyStubClsid32\ Value: None		2560
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		2560
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		2560
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		2560
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		2560
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		2560
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		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\ Value: None		2560
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		2560
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		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\ProxyStubClsid32\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\ProxyStubClsid32\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\ProxyStubClsid32\(Default) Value: None		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\TypeLib\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\TypeLib\(Default) Value: None		2560

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\TypeLib\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A5}\TypeLib\Version Value: 1.2		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\(Default) Value: None		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\ProxyStubClsid32\ Value: None		2560
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		2560
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		2560
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		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\TypeLib\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\TypeLib\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6A6}\TypeLib\Version Value: 1.2		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\(Default) Value: None		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\ProxyStubClsid32\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\ProxyStubClsid32\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\ProxyStubClsid32\(Default) Value: None		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{5073BDEB-E480-4024-887E-22923C004444}\TypeLib\ Value: None		2560
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		2560
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		2560
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		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\ Value: None		2560
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		2560
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		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\ProxyStubClsid32\ Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\ProxyStubClsid32\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\ProxyStubClsid32\(Default) Value: None		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\TypeLib\ Value: None		2560
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		2560
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		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{FE6A04A8-6CE8-449F-87F1-1AFB705547AE}\TypeLib\Version Value: 1.2		2560
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\ Value: None		2560
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		2560
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		2560
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		2560
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		2560
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		2560
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		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\TypeLib\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\TypeLib\(Default) Value: None		2560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9BF068D0-B736-11D3-B2CF-00500489D6D6}\TypeLib\Version Value: 1.2		2560
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\ Value: None		2560

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\ Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\FriendlyName Value: Microsoft Excel		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\LabelText Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\Save Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\ShowButtons Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\ShowIndicators Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\NoLabelOption Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\NoSaveOption Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\NoButtonOption Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN\NoIndicatorOption Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D2FED\1D2FED Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D2FED\ Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2560
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ImmersiveWorkbookDirtySentinel Value: 7fffffff		2560
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\41FFA142.png Type: VSDT_PNG		2560
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\41FFA142.png Type: VSDT_PNG		2560
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\41FFA142.png Type: VSDT_PNG		2560
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2560
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -1780450624) Return: cc0008		2560
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -1767182744, -2067004672, -1780450624) Return: cc000c		2560
Call System API	API Name: WinHttpCloseHandle Args: (95f8ad50) Return: 1		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: df8		2560
Call Network API	API Name: bind Args: (df8, 0.0.0.0:49180, 16) Return: 0		2560
Call System API	API Name: ConnectEx Args: (df8, self.events.data.microsoft.com:443, 16, 0, 0, 0, 921eb378) Return: 0		2560
Call Network API	API Name: send Args: (df8, ..., 1, 191) Return: 0		2560
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2560\0 Value: None		2560
Call System API	API Name: WinHttpCloseHandle Args: (95f8c820) Return: 1		2560
Call Network API	API Name: socket Args: (2, 2, 0) Return: de4		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: de4		2560
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2560
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2560
Call Network API	API Name: socket Args: (23, 2, 0) Return: 250		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1078		2560
Call Network API	API Name: bind Args: (1078, 0.0.0.0:49181, 128) Return: 0		2560
Call System API	API Name: ConnectEx Args: (1078, ctldl.windowsupdate.com:80, 16, 0, 0, 0, 9606bc08) Return: 0		2560
Call Network API	API Name: send Args: (1078, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?370a6a6898a557ea 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		2560
Call System API	API Name: WinHttpCloseHandle Args: (8ea422d0) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (9606b670) Return: 1		2560
Call System API	API Name: WinHttpCloseHandle Args: (960d3cb0) Return: 1		2560
Call Filesystem API	API Name: RemoveDirectoryW Args: (%TEMP%\{5970A11A-B0C4-4BEE-BBF9-DBE35D6F6EF9}\ ) Return: 1		2560
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\40056F05.emf) Return: 1		2560
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2560
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -1780462768) Return: cc0008		2560
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -1767182744, -2067004672, -1780462768) Return: cc000c		2560
Call Network API	API Name: socket Args: (2, 1, 6) Return: dc8		2560
Call Network API	API Name: bind Args: (dc8, 0.0.0.0:49182, 16) Return: 0		2560
Call System API	API Name: ConnectEx Args: (dc8, self.events.data.microsoft.com:443, 16, 0, 0, 0, 921eb8b8) Return: 0		2560
Call Network API	API Name: send Args: (dc8, ..., 1, 191) Return: 0		2560

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	5D9887AF2E228247570142E1CDB42BE7A8DCEBF1
SHA-256	6ADAA8243CC0677C23674C2CDD90ED767FF86642795801DB2A9D49E6ADBFA549
MD5	3DD1DDC729C809AEA00DD366BE58B3B2
Size	127561 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

Network Destinations

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

URL	Site Category	Risk Level	Threat	Accessed By
https://augmentation.osi.office.net/officeaugmentation/searchendpoint/	Computers / Internet	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm
https://self.events.data.microsoft.com/OneCollector/1.0/	Business / Economy Computers / Internet Cloud Applications	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
winword.exe.db-shm	No risk	-	-	-	32768	7A661AE8F4758104E68DDC5B62ACE9757D1DFABF
~$Normal.dotm	No risk	-	-	-	162	BE995D4573DC600AC0AC8E8A8842EB347C3CB41B
~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx	No risk	-	-	-	162	D8DCBC82B334EBBDF81F8BA977CCDAEA01FF4F73
~WRS{FBD12C91-4D0F-4CB8-A074-563DCDCB034A}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
winword.exe.db-wal	No risk	-	-	-	4152	B9AC334FB2F272B652044A7B1FFFA6964312703E
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	302	CB400EC3C4DA26864862CB5348AB77D8F6F25735
{D618020A-E2E2-4EB3-A342-E81E9AEDC8AF} - OProcSessId.dat	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
App_16139876319317058 00_D618020A-E2E2-4EB3-A342-E81E9AEDC8AF.log	No risk	-	-	-	20971520	9674344C90C2F0646F0B78026E127C9B86E3AD77
App_16139876319303818 00_D618020A-E2E2-4EB3-A342-E81E9AEDC8AF.log	No risk	-	-	-	20971520	0EB4D0D707D86A6A83A7C2A9257480AA5504FFB4

Analysis

Event Type	Details	Parent PID	PID
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ClientTelemetry\Sampling\0 Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2604\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2604\0 Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\ Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\z}! Value: None		2604
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\Diagnostics\WINWORD\App_1600985251099791600_A16BA699-DE8A-473F-B54F-C8D59B3C1D07.log) Return: 1		2604
Delete File	Path: %TEMP%\Diagnostics\WINWORD\App_1600985251099791600_A16BA699-DE8A-473F-B54F-C8D59B3C1D07.log Type: VSDT_EMPTY		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2532\0 Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2532\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2604\0 Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\4 Value: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\Categories Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\4 Value: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\Categories Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ULSAllCategories Value: 6, 10		2604
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, 8589f6d0) Return: 0		2604
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 8589f6d0) Return: 0		2604
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 8589f610) Return: 0		2604
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0		2604
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, 8589f610) Return: 0		2604
Call WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0		2604
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, 8589f610) Return: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\f\52C64B7E\LanguageList Value: en-US\0en\0		2604

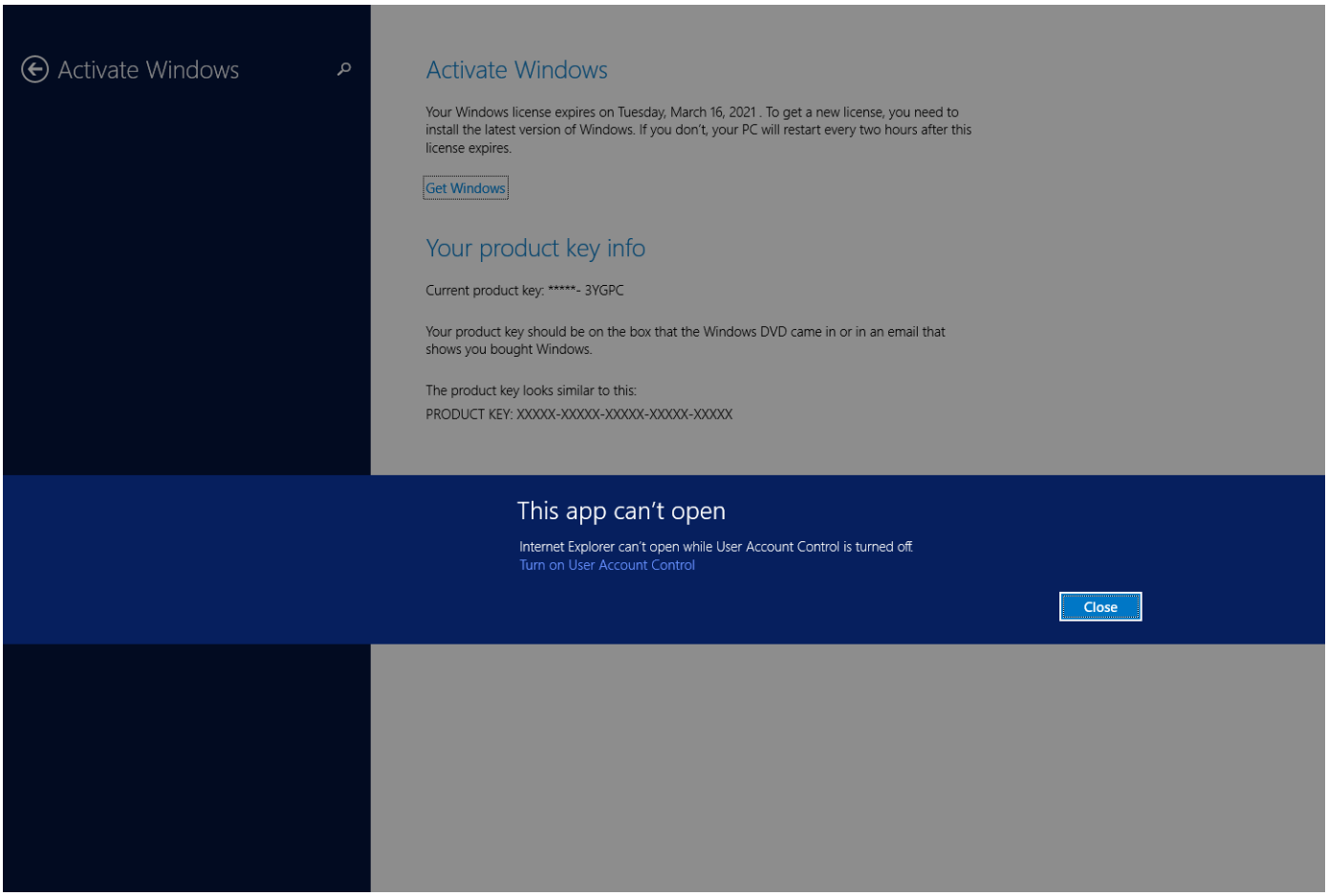
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, 85aae060) Return: 0		2604
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 85aae060) Return: 0		2604
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 85aadfa0) Return: 0		2604
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0		2604
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, 85aadfa0) Return: 0		2604
Call WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0		2604
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, 85aadfa0) Return: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\h*" Value: None		2604
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2604
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\h*" Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastSyncTimeWord Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastWriteTimeWord Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2604\0 Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\$." Value: None		2604
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx) Return: 1		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\$." Value: None		2604
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\z}! Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2604\0 Value: None		2604
Call Network API	API Name: socket Args: (2, 2, 0) Return: a2c		2604
Call Network API	API Name: bind Args: (a2c, 127.0.0.1:52397, 128) Return: 0		2604
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (8589e570, 0, 0, 0) Return: 1		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2604
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0004		2604
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (8589e410, 0, 0, 0) Return: 1		2604
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (8589e3e0, 0, 0, 0) Return: 1		2604
Call Network API	API Name: socket Args: (23, 1, 6) Return: ae8		2604
Call Network API	API Name: socket Args: (2, 1, 0) Return: a68		2604
Call Network API	API Name: socket Args: (23, 1, 6) Return: b5c		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\SessionId Value: None		2604
Call System API	API Name: WinHttpCloseHandle Args: (fdad48c0) Return: 1		2604
Call Network API	API Name: socket Args: (23, 1, 6) Return: bb4		2604
Call System API	API Name: WinHttpCloseHandle Args: (fdad48c0) Return: 1		2604
Call Network API	API Name: socket Args: (2, 2, 0) Return: c24		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: c24		2604
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87		2604
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: c2c		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: c2c		2604
Call Network API	API Name: bind Args: (c2c, 0.0.0.0:49168, 128) Return: 0		2604
Call System API	API Name: ConnectEx Args: (c2c, gmail.com:443, 16, 0, 0, 0, 8e17fd98) Return: 0		2604
Call Network API	API Name: send Args: (c2c, ..., 1, 170) Return: 0		2604
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		2604
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2604
Call System API	API Name: WinHttpCloseHandle Args: (fd850520) Return: 1		2604
Call System API	API Name: WinHttpCloseHandle Args: (8e1801a0) Return: 1		2604
Call Network API	API Name: socket Args: (2, 2, 0) Return: c2c		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: c2c		2604
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1, 40006000) Return: 87		2604
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1c, 40026000) Return: 9003		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: c38		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: c38		2604
Call Network API	API Name: bind Args: (c38, 0.0.0.0:49169, 128) Return: 0		2604
Call System API	API Name: ConnectEx Args: (c38, autodiscover.gmail.com:443, 16, 0, 0, 0, 8e17f6b8) Return: 0		2604
Call Network API	API Name: send Args: (c38, ..., 1, 183) Return: 0		2604
Call System API	API Name: WinHttpCloseHandle Args: (8ddfff20) Return: 1		2604
Call System API	API Name: WinHttpCloseHandle Args: (8e17ed00) Return: 1		2604
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2604
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -2023266512) Return: cc0008		2604
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -1861946808, -2067004672, -2023266512) Return: cc000c		2604

Call Network API	API Name: socket Args: (2, 2, 0) Return: e5c		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: e5c		2604
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87		2604
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: e60		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: e60		2604
Call Network API	API Name: bind Args: (e60, 0.0.0.0:49170, 16) Return: 0		2604
Call System API	API Name: ConnectEx Args: (e60, self.events.data.microsoft.com:443, 16, 0, 0, 0, 8df55618) Return: 0		2604
Call Network API	API Name: send Args: (e60, ..., 1, 191) Return: 0		2604
Call System API	API Name: WinHttpCloseHandle Args: (fd9def40) Return: 1		2604
Call Network API	API Name: socket Args: (2, 2, 0) Return: ed4		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: ed4		2604
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2604
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: e58		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: e58		2604
Call Network API	API Name: bind Args: (e58, 0.0.0.0:49171, 128) Return: 0		2604
Call System API	API Name: ConnectEx Args: (e58, ctldl.windowsupdate.com:80, 16, 0, 0, 0, 8e17e0b8) Return: 0		2604
Call Network API	API Name: send Args: (e58, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?fa5141e88f73eaa4 HTTP/1.1\r\nConnection: Keep-Alive\r\n Accept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0		2604
Call System API	API Name: WinHttpCloseHandle Args: (8ddfff20) Return: 1		2604
Call System API	API Name: WinHttpCloseHandle Args: (8e17fd80) Return: 1		2604
Call System API	API Name: WinHttpCloseHandle Args: (8e0db990) Return: 1		2604
Call Network API	API Name: socket Args: (23, 1, 6) Return: eb8		2604
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0008		2604
Call System API	API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003		2604
Call Internet Helper API	API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c		2604
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc000c, GET, /officeaugmentation/searchendpoint/, , , 0, -2134884352, -1950338288) Return: cc0010		2604
Call Network API	API Name: socket Args: (2, 2, 0) Return: edc		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: edc		2604
Call System API	API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1c, 40026000) Return: 9003		2604
Call System API	API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 40006000) Return: 87		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: f04		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: edc		2604
Call Network API	API Name: bind Args: (edc, 0.0.0.0:49172, 16) Return: 0		2604
Call System API	API Name: ConnectEx Args: (edc, augmentation.osi.office.net:443, 16, 0, 0, 0, 8df54348) Return: 0		2604
Call Network API	API Name: send Args: (edc, ..., 1, 188) Return: 0		2604
Call System API	API Name: WinHttpCloseHandle Args: (fd9def40) Return: 1		2604
Call Network API	API Name: socket Args: (2, 2, 0) Return: ef8		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: ef8		2604
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2604
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: ef8		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: ef8		2604
Call Network API	API Name: bind Args: (ef8, 0.0.0.0:49173, 128) Return: 0		2604
Call System API	API Name: ConnectEx Args: (ef8, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 8e17f138) Return: 0		2604
Call Network API	API Name: send Args: (ef8, ..., 1, 188) Return: 0		2604
Call System API	API Name: WinHttpCloseHandle Args: (8ddfff20) Return: 1		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: ef8		2604
Call Network API	API Name: bind Args: (ef8, 0.0.0.0:49174, 128) Return: 0		2604
Call System API	API Name: ConnectEx Args: (ef8, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 8e180898) Return: 0		2604
Call Network API	API Name: send Args: (ef8, ..., 1, 188) Return: 0		2604
Call System API	API Name: WinHttpCloseHandle Args: (8ddff0e0) Return: 1		2604
Call System API	API Name: WinHttpCloseHandle Args: (8e181640) Return: 1		2604
Call System API	API Name: WinHttpCloseHandle Args: (8e180ca0) Return: 1		2604
Call System API	API Name: WinHttpCloseHandle Args: (fd9e0ef0) Return: 1		2604
Call Network API	API Name: socket Args: (2, 2, 0) Return: f1c		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: f1c		2604
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2604
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: ee8		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: ee8		2604
Call Network API	API Name: bind Args: (ee8, 0.0.0.0:49175, 128) Return: 0		2604
Call System API	API Name: ConnectEx Args: (ee8, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 8e17f3f8) Return: 0		2604
Call Network API	API Name: send Args: (ee8, ..., 1, 188) Return: 0		2604
Call System API	API Name: WinHttpCloseHandle Args: (8ddfff20) Return: 1		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: ee8		2604
Call Network API	API Name: bind Args: (ee8, 0.0.0.0:49176, 128) Return: 0		2604
Call System API	API Name: ConnectEx Args: (ee8, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 8e17ed18) Return: 0		2604
Call Network API	API Name: send Args: (ee8, ..., 1, 188) Return: 0		2604
Call System API	API Name: WinHttpCloseHandle Args: (8ddff0e0) Return: 1		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: ee8		2604

Call Network API	API Name: bind Args: (ee8, 0.0.0.0:49177, 128) Return: 0		2604
Call System API	API Name: ConnectEx Args: (ee8, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 8e17f3f8) Return: 0		2604
Call Network API	API Name: send Args: (ee8, ..., 1, 188) Return: 0		2604
Call System API	API Name: WinHttpCloseHandle Args: (8ddfff20) Return: 1		2604
Call System API	API Name: WinHttpCloseHandle Args: (8e180b40) Return: 1		2604
Call System API	API Name: WinHttpCloseHandle Args: (8e17f800) Return: 1		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: ee8		2604
Call Network API	API Name: bind Args: (ee8, 0.0.0.0:49178, 128) Return: 0		2604
Call System API	API Name: ConnectEx Args: (ee8, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 8e17e0b8) Return: 0		2604
Call Network API	API Name: send Args: (ee8, ..., 1, 188) Return: 0		2604
Call System API	API Name: WinHttpCloseHandle Args: (8ddff0e0) Return: 1		2604
Call System API	API Name: WinHttpCloseHandle Args: (8e17f280) Return: 1		2604
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2604
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -2023280864) Return: cc0008		2604
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -1861946808, -2067004672, -2023280864) Return: cc000c		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: e58		2604
Call Network API	API Name: bind Args: (e58, 0.0.0.0:49179, 16) Return: 0		2604
Call System API	API Name: ConnectEx Args: (e58, self.events.data.microsoft.com:443, 16, 0, 0, 0, 8df563a8) Return: 0		2604
Call Network API	API Name: send Args: (e58, ..., 1, 191) Return: 0		2604
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2604
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -2023266512) Return: cc0008		2604
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -1861946808, -2067004672, -2023266512) Return: cc000c		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: e58		2604
Call Network API	API Name: bind Args: (e58, 0.0.0.0:49180, 16) Return: 0		2604
Call System API	API Name: ConnectEx Args: (e58, self.events.data.microsoft.com:443, 16, 0, 0, 0, 8df56e28) Return: 0		2604
Call Network API	API Name: send Args: (e58, ..., 1, 191) Return: 0		2604
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2604
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -2023270928) Return: cc0008		2604
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -1861946808, -2067004672, -2023270928) Return: cc000c		2604
Call System API	API Name: WinHttpCloseHandle Args: (fd9dea60) Return: 1		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: f14		2604
Call Network API	API Name: bind Args: (f14, 0.0.0.0:49181, 16) Return: 0		2604
Call System API	API Name: ConnectEx Args: (f14, self.events.data.microsoft.com:443, 16, 0, 0, 0, 8df55768) Return: 0		2604
Call Network API	API Name: send Args: (f14, ..., 1, 191) Return: 0		2604
Call System API	API Name: WinHttpCloseHandle Args: (fd9dfb70) Return: 1		2604
Call Network API	API Name: socket Args: (2, 2, 0) Return: f28		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: f28		2604
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2604
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2604
Call Network API	API Name: socket Args: (23, 2, 0) Return: f1c		2604
Call Network API	API Name: socket Args: (2, 1, 6) Return: f1c		2604
Call Network API	API Name: bind Args: (f1c, 0.0.0.0:49182, 128) Return: 0		2604
Call System API	API Name: ConnectEx Args: (f1c, ctldl.windowsupdate.com:80, 16, 0, 0, 0, 8e17f138) Return: 0		2604
Call Network API	API Name: send Args: (f1c, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?865270441ffadb00 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		2604
Call System API	API Name: WinHttpCloseHandle Args: (8ddfff20) Return: 1		2604
Call System API	API Name: WinHttpCloseHandle Args: (8e17fac0) Return: 1		2604
Call System API	API Name: WinHttpCloseHandle Args: (8e0db1d0) Return: 1		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Toolbars\Settings\Microsoft Word Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\5 Value: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\Categories Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\4 Value: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\Categories Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\5 Value: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\Categories Value: None		2604

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\4 Value: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\Categories Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\4 Value: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\Categories Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ULSAllCategories Value: 6, 10		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security\Trusted Documents\LastPurgeTime Value: 19a7552		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2604
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\5 Value: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\Categories Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\4 Value: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\Categories Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\5 Value: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\Categories Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\4 Value: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\Categories Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\4 Value: 0		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\Categories Value: None		2604
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2604
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ULSAllCategories Value: 6, 10		2604

▼ Screenshot



Process Graph Legend