

# Virtual Analyzer Report



## Submission Context

Logged	2021-03-20 12:44:11
Submitter	Manual Submission
Type	MS OLE document

## Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	TROJ_FRS.0NA103C821		
Exploited vulnerabilities	-		
Analyzed objects	MS OLE document	1 - RF-E68-STD-081.xlsx	0477AD566347E79C96B79CBE3BC44AE9B4EDCEF2
	Office Excel 2007 spreadsheet	1.1 - NONAMEFL	1B87A12587E64C861DD1BC2393D98A295FDC5475
	Office Word 2007 document	1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm	738E9370EF36110EA752304C9BBC67EFE043ED47

## Analysis Environments

	Win2012_Office
Anti-security, self-preservation	
Autostart or other system reconfiguration	
Deception, social engineering	
File drop, download, sharing, or replication	✓
Hijack, redirection, or data theft	✓
Malformed, defective, or with known malware traits	✓
Process, service, or memory object change	
Rootkit, cloaking	
Suspicious network or messaging activity	✓

## Win2012\_Office

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

### Object 1 - RF-E68-STD-081.xlsx (MS OLE document)

File name	RF-E68-STD-081.xlsx
File type	MS OLE document
SHA-1	0477AD566347E79C96B79CBE3BC44AE9B4EDCEF2
SHA-256	2C0625D46A85F0CF4B43E08ABE30CB4EA591CC0A84D9414EC21FDA75BEF47484
MD5	F0A960B15283F180E599491EB1E56BE7
Size	2355712 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.0NA103C821
Exploited vulnerabilities	-
Threat Characteristics	File drop, download, sharing, or replication (2) Hijack, redirection, or data theft (3) Malformed, defective, or with known malware traits (1) Suspicious network or messaging activity (14)

## Process Graph



Process Graph Legend

## MITRE ATT&CK™ Framework Tactics and Techniques

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

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

### Notable Threat Characteristics

File drop, download, sharing, or replication (2)

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 2424 File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\FB84CAC1.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 2424 File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\7B6031CE.jpeg Type: VSDT_JPG

▼ Hijack, redirection, or data theft (3)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2424 Info: Enums share folder from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2424 Info: Obtains Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%' from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2424 Info: Obtains Win32_ComputerSystemProduct from API result

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

Characteristic	Significance	Details
Detected as known malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: TROJ_FRS.0NA103C821 Engine Version: 12.500.1008 Malware Pattern Version: 16.603.92

▼ Suspicious network or messaging activity (14)

Characteristic	Significance	Details
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49178
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49177
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49176
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49175
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49174
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49173
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49172
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49171
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49170
Listens on port	<div><div></div><div></div><div></div></div>	127.0.0.1:65200
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49169
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49168
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49167
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49166

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
gmail.com	-	53	-	No risk	-	RF-E68-STD-081.xlsx
clients2.google.com	-	53	-	No risk	-	RF-E68-STD-081.xlsx
self.events.data.microsoft.com	-	53	-	No risk	-	RF-E68-STD-081.xlsx
ctldl.windowsupdate.com	-	53	-	No risk	-	RF-E68-STD-081.xlsx
www.msftncsi.com	-	53	-	No risk	-	RF-E68-STD-081.xlsx
cdn.uci.officeapps.live.com	-	53	-	No risk	-	RF-E68-STD-081.xlsx
autodiscover.gmail.com	-	53	-	No risk	-	RF-E68-STD-081.xlsx
autodiscover.gmail.com	-	443	-	No risk	-	RF-E68-STD-081.xlsx
gmail.com	-	443	-	No risk	-	RF-E68-STD-081.xlsx

URL	Site Category	Risk Level	Threat	Accessed By
https://self.events.data.microsoft.com/OneCollect or/1.0/	Business / Economy Computers / Internet Cloud Applications	No risk	-	RF-E68-STD-081.xlsx

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
91O6TLGSSSW5AIPSW0Z3.tem p	No risk	-	-	-	7682	3AA28605F3E7260CBDECEA57D7641E0BAF3385E6
excel.exe.db-shm	No risk	-	-	-	32768	B5059A849A52CFA67CA321E5EC6D10C8B99315A9
~\$RF-E68-STD-081.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
b8ab77100df80ab2.customDestin ations-ms	No risk	-	-	-	7682	3AA28605F3E7260CBDECEA57D7641E0BAF3385E6
~DF382CF3092AC89FD4.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD 7ED4AE5
excel.exe.db-wal	No risk	-	-	-	4152	4D10FA1BB2A8F1C3F8871D017E2FEA2428 588893
57C8EDB95DF3F0AD4EE2DC2B 8CFD4157	No risk	-	-	-	302	8F37D12D79E25FC68E017C2A3D94CE6948 6B05E7
7B6031CE.jpeg	No risk	-	-	-	45677	4545D7788B69E441BDCD8B2A667ED5B599 85E12B
FB84CAC1.png	No risk	-	-	-	79394	9F3FE15AE44644F9ED8C2CA668B7020DF7 26426B
hostproperties.json	No risk	-	-	-	185	BC583C6DD14A35DA17CF1197B25D3A0E4 B4D83BF

▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	0477AD566347E79C96B79CBE3BC44AE9B4EDCEF2	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.0NA103C821 Engine Version: 12.500.1008 Malware Pattern Version: 16.603.92		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ClientTelemetry\Sampling\1 Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2424\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2424\0 Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\?>& Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ImmersiveWorkbookDirtySentinel Value: 0		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ExcelWorkbookOpenedCount Value: 0		2424
Call Filesystem API	API Name: DeleteFileW Args: ( %TEMP%\Diagnostics\EXCEL\App_1600985250979406400_37DFED58-65EC-4733-9903-AF526D736AF9.log ) Return: 1		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\EXCEL\2704\0 Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\EXCEL\2704\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2424\0 Value: None		2424
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: ( ROOT\CIMV2, en-US,en, 0, 0, eb7ff3a0 ) Return: 0		2424
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, eb7ff3a0 ) Return: 0		2424
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, eb7ffe0 ) Return: 0		2424
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2424 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		2424
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE "%PHYSICALDRIVE0%", 30, 0, eb7ffe0 ) Return: 0		2424
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2424 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		2424
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag=Physical Memory 0', 30, 0, eb7ffe0 ) Return: 0		2424
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\1f52C64B7E\LanguageList Value: en-US\0en\0		2424
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: ( ROOT\CIMV2, en-US,en, 0, 0, eb7fe0f0 ) Return: 0		2424
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, eb7fe0f0 ) Return: 0		2424
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, eb7fe030 ) Return: 0		2424
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: ( UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0 ) Return: 0		2424
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE "%PHYSICALDRIVE0%", 30, 0, eb7fe030 ) Return: 0		2424
Call WMI API	API Name: Win32_DiskDrive::Get Args: ( SerialNumber, 0, GJZ3J0NSM, 0, 0 ) Return: 0		2424
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag=Physical Memory 0', 30, 0, eb7fe030 ) Return: 0		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\?>& Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2424

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastSyncTimeExcel Value: None	2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastWriteTimeExcel Value: None	2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None	2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None	2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\w-& Value: None	2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None	2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CB956\ Value: None	2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CB956\1CB956 Value: None	2424
Call System API	API Name: CryptDeriveKey Args: ( efcabe60, 660e, efd9ae60, 800000, e1998f40 ) Return: 1	2424
Call System API	API Name: CryptDeriveKey Args: ( efcabe60, 660e, efd9ae40, 800000, efc3638 ) Return: 1	2424
Call System API	API Name: CryptDeriveKey Args: ( efcabe60, 660e, efd99a20, 800000, efc3638 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, 5f6dGä..?/Ó©'üz, 16, 0, , 0, 5f6dGä..?/Ó©'üz, 16, -510029136, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, e19992e8, 10 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, [  ], 32, 0, , 0, [  ], 32, -510029136, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd09520, 20 ) Return: 1	2424
Call System API	API Name: CryptDeriveKey Args: ( efcad960, 660e, efd9b2a0, 800000, efc359d8 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, PK, 4096, 0, , 0, PK, 4096, -510028112, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, , 2640, 0, , 0, , 2640, -510029888, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, a50 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, PK, 4096, 0, , 0, PK, 4096, -510032448, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ExcelWorkbookOpenedCount Value: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, œ&]ñ, 4096, 0, , 0, œ&]ñ, 4096, -510039680, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20,  F", 4096, 0, , 0,  F", 4096, -510039680, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, Š'ÁZÓĈE:wíòä, 4096, 0, , 0, Š'ÁZÓĈE:wíòä, 4096, -510039680, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, äÄ'S!\$!Övßj+YŸY!×'tM%izlÖ6N, l'S!\$%öi-ß%úñüëYwßjóš7¿ üòµ%-ø öiEIQXlkð>ëY'^xñhé«~¿zzZ/i...kiä?~%J k×\$þ+ÿ+ÿ?ýÖ?ÿyl+Ç%kpbwpyl=Z", 4096, 0, , 0, äÄ'S!\$!Övßj+YŸY!×'tM%izlÖ6N, l'S!\$%öi-ß%úñüëYwßjóš7¿ üòµ%-ø öiEIQXlkð>ëY'^xñhé«~¿zzZ/i...kiä?~%J k×\$þ+ÿ+ÿ?ýÖ?ÿyl+Ç%kpbwpyl=Z", 4096, -510039680, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, +, 4096, 0, , 0, +, 4096, -510039680, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, , 4096, 0, , 0, , 4096, -510039712, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, ÿlc, 4096, 0, , 0, ÿlc, 4096, -510039680, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, , 2640, 0, , 0, , 2640, -510040752, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, a50 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, PK, 4096, 0, , 0, PK, 4096, -510039376, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CB956\1CB956 Value: None	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, +, 4096, 0, , 0, +, 4096, -510039456, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20,  F", 4096, 0, , 0,  F", 4096, -510045248, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, ÿlc, 4096, 0, , 0, ÿlc, 4096, -510043760, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20,  F", 4096, 0, , 0,  F", 4096, -510076432, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, œ&]ñ, 4096, 0, , 0, œ&]ñ, 4096, -510074992, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, , 4096, 0, , 0, , 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, Úw, 4096, 0, , 0, Úw, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: CryptDecrypt Args: ( efd9a7b0, 0, 0, 0, efd9e6cc, 1000 ) Return: 1	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, ÁYëAH@FL, 4096, 0, , 0, ÁYëAH@FL, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, ié@FÇ, 4096, 0, , 0, ié@FÇ, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, ;+9, 4096, 0, , 0, ;+9, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, 3, 4096, 0, , 0, 3, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, Ä~ñl")Ötğ., 4096, 0, , 0, Ä~ñl")Ötğ., 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, ä'nln<«è, 4096, 0, , 0, ä'nln<«è, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, ..., 4096, 0, , 0, ..., 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, ), 4096, 0, , 0, ), 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, l~f, 4096, 0, , 0, l~f, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, ýRAID@tš«ç3c;±, 4096, 0, , 0, ýRAID@tš«ç3c;±, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, mTñ×?+yóÊÇ, 4096, 0, , 0, mTñ×?+yóÊÇ, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, —Ö«, 4096, 0, , 0, —Ö«, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, , 4096, 0, , 0, , 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, iéëlrğ, 4096, 0, , 0, iéëlrğ, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efd4a4b20, €, 4096, 0, , 0, €, 4096, -510075024, 0 ) Return: 0	2424

Call System API	API Name: BCryptDecrypt Args: ( efda4b20, {0{kuu"Öq"}@kk<Ká:9@—†, 4096, 0, , 0, {0{kuu"Öq"}@kk<Ká:9@—†, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, RÊÇŸóí?¿-lnĖ.a, s6", 4096, 0, , 0, RÊÇŸóí?¿-lnĖ.a, s6", 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, , Í<"=F4Qbe, 4096, 0, , 0, , Í<"=F4Qbe, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ÁúĹ-Gh, 4096, 0, , 0, ÁúĹ-Gh, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ôĖu0pXl)0Ç, 4096, 0, , 0, ôĖu0pXl)0Ç, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, \$ @'ÇD, 4096, 0, , 0, \$ @'ÇD, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, à8+mf, 4096, 0, , 0, à8+mf, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, , 4096, 0, , 0, , 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, úBú, 4096, 0, , 0, úBú, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, k3, 4096, 0, , 0, k3, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, i"Ā.óí?_ë"e.ŸĪĪ, 4096, 0, , 0, i"Ā.óí?_ë"e.ŸĪĪ, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, 'µŬ -, 4096, 0, , 0, 'µŬ -, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, Ā'gLEæ2āZ, 4096, 0, , 0, Ā'gLEæ2āZ, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, Ćë', 4096, 0, , 0, Ćë', 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, w=ŕŕkĹLžiz-aa-q:v0Ė:io×"ĖhÇvg, 4096, 0, , 0, w=ŕŕkĹLžiz-aa-q:v0Ė:io×"ĖhÇvg, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, xŷ¬, 4096, 0, , 0, xŷ¬, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, â1¼%ô, 4096, 0, , 0, â1¼%ô, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, 'M¼"Īŕ dxlôžâ)3±=N"oĖ+7 ç0Ÿpâ, 4096, 0, , 0, 'M¼"Īŕ dxlôžâ)3±=N"oĖ+7 ç0Ÿpâ, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ¬xŷÇ7\Ç, 4096, 0, , 0, ¬xŷÇ7\Ç, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, DL¼, 4096, 0, , 0, DL¼, 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, , 4096, 0, , 0, , 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20,  F", 4096, 0, , 0,  F", 4096, -510075024, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, , 4096, 0, , 0, , 4096, -510040848, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20,  F", 4096, 0, , 0,  F", 4096, -510058544, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, Š"ĀZŎĖ:włôâ, 4096, 0, , 0, Š"ĀZŎĖ:włôâ, 4096, -510044032, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, •NĪ-q4[<@o"ôk"ôÜGiĀĪ , 4096, 0, , 0, •NĪ-q4[<@o"ôk"ôÜGiĀĪ , 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, 8:7, 4096, 0, , 0, 8:7, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, kô>2Vy"Žú, 4096, 0, , 0, kô>2Vy"Žú, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, pĀĹø8lŎúô, 4096, 0, , 0, pĀĹø8lŎúô, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ĆE-&ŎĖqia, 4096, 0, , 0, ĆE-&ŎĖqia, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ,, 4096, 0, , 0, ,, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, i"¢Ė, 4096, 0, , 0, i"¢Ė, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, žŎÇ:ŷŷŬB-úâ, 4096, 0, , 0, žŎÇ:ŷŷŬB-úâ, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, »), 4096, 0, , 0, »), 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, Šýô"ĪİŠ, 4096, 0, , 0, Šýô"ĪİŠ, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, Ÿgl, 4096, 0, , 0, Ÿgl, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, Ŭ±)žŎÇ:ŷŷŬB-ú, 4096, 0, , 0, Ŭ±)žŎÇ:ŷŷŬB-ú, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, úø6"_, 4096, 0, , 0, úø6"_, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ĩ, 4096, 0, , 0, ĩ, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, , 4096, 0, , 0, , 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ~, IsUœüŎüñ, 4096, 0, , 0, ~, IsUœüŎüñ, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, V:Žŷm."™êlsj, 4096, 0, , 0, V:Žŷm."™êlsj, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, àð+, 4096, 0, , 0, àð+, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, -uŎJL, 4096, 0, , 0, -uŎJL, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, àĀ'\$!\$!Ŏvŝ)+ŸŸY!×"tM%izlŎ6N, I'\$!\$%ô!-B34úñûĖYwŝyôŝ7%jûôp%-ŎlôlĖIQXlôkô>ëY^^xñĕ"~%zz/!..kiâ?~%3J K×\$p~y+îŸ?ôŸyyl+Ç%kpwpy=ž?), 4096, 0, , 0, àĀ'\$!\$!Ŏvŝ)+ŸŸY!×"tM%izlŎ6N, I'\$!\$%ô!-B34úñûĖYwŝyôŝ7%jûôp%-ŎlôlĖIQXlôkô>ëY^^xñĕ"~%zz/!..kiâ?~%3J K×\$p~y+îŸ?ôŸyyl+Ç%kpwpy=ž?), 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20,  F", 4096, 0, , 0,  F", 4096, -510044032, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ŭŦŭŬJ"d, 4096, 0, , 0, ŭŦŭŬJ"d, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, %NŦlĀ)peĖĖġg"æt"PS>MŬŎœt-ŸQ_İŝu??ôœy, 4096, 0, , 0, %NŦlĀ)peĖĖġg"æt"PS>MŬŎœt-ŸQ_İŝu??ôœy, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ŬžXô"Ž-, 4096, 0, , 0, ŬžXô"Ž-, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, N"Ŧ"-=ŁŮT??"-ôS6\$, 4096, 0, , 0, N"Ŧ"-=ŁŮT??"-ôS6\$, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, U, 4096, 0, , 0, U, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, %Ææ", 4096, 0, , 0, %Ææ", 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, hás*ŬŎj+îŦNôj<«t!ô@+~ĲĖŸ#±ø×@ê%!Ŏm-<6—V"Ŏ"mô, 4096, 0, , 0, hás*ŬŎj+îŦNôj<«t!ô@+~ĲĖŸ#±ø×@ê%!Ŏm-<6—V"Ŏ"mô, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, Ŧj)lâ"Ŏ%&9, 4096, 0, , 0, Ŧj)lâ"Ŏ%&9, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, × x, 4096, 0, , 0, × x, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ðo7qŸĹÆ"Ĳ...ŷ, 4096, 0, , 0, ðo7qŸĹÆ"Ĳ...ŷ, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, Š"ĀZŎĖ:włôâ, 4096, 0, , 0, Š"ĀZŎĖ:włôâ, 4096, -510044064, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, , 4096, 0, , 0, , 4096, -510045536, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, a, 4096, 0, , 0, a, 4096, -510045568, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, 'C%="A, 4096, 0, , 0, 'C%="A, 4096, -510045568, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, Čô, 4096, 0, , 0, Čô, 4096, -510045568, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, pãš, 4096, 0, , 0, pãš, 4096, -510045568, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, Ā~s74)D"ċ""m,zà«, 4096, 0, , 0, Ā~s74)D"ċ""m,zà«, 4096, -510045568, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, %šai ŎlŠâ"â.)rš)Ÿ ħL, 4096, 0, , 0, %šai ŎlŠâ"â.)rš)Ÿ ħL, 4096, -510045568, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, , 4096, 0, , 0, , 4096, -510045568, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ôŎ, 4096, 0, , 0, ôŎ, 4096, -510045568, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, €, 4096, 0, , 0, €, 4096, -510045568, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, C+8Ů7Ł, 4096, 0, , 0, C+8Ů7Ł, 4096, -510045568, 0 ) Return: 0	2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, v, 4096, 0, , 0, v, 4096, -510045568, 0 ) Return: 0	2424

Call System API	API Name: BCryptDecrypt Args: ( efda4b20, iä, 4096, 0, , 0, iä, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, -, 4096, 0, , 0, -, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, >1Â[âAö^Y%öJ, 4096, 0, , 0, >1Â[âAö^Y%öJ, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, éliëçq1"d%ì /E=ÜVl%, 4096, 0, , 0, éliëçq1"d%ì /E=ÜVl%, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, æê*ráð ¿€ƒ, 4096, 0, , 0, æê*ráð ¿€ƒ, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ŠVÖÖ",6:x@ ""iL0 iZ, 4096, 0, , 0, ŠVÖÖ",6:x@ ""iL0 iZ, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20,  Êœæææ CldY% 'o, 4096, 0, , 0,  Êœæææ CldY% 'o, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, , 4096, 0, , 0, , 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, , 4096, 0, , 0, , 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ÜÖ±ø!r%œ&*f, 4096, 0, , 0, ÜÖ±ø!r%œ&*f, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, , 4096, 0, , 0, , 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ,Ä(»ÖœÜÐÄsOÄ, 4096, 0, , 0, ,Ä(»ÖœÜÐÄsOÄ, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, \$U, 4096, 0, , 0, \$U, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, kYlMcIn, 4096, 0, , 0, kYlMcIn, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, Cyî-jà1UJ^Ö, 4096, 0, , 0, Cyî-jà1UJ^Ö, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, *üD¿!ø_!=flÿt%MlY@ÄiÊ@], 4096, 0, , 0, *üD¿!ø_!=flÿt%MlY@ÄiÊ@], 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, V\rGq†â!XÊµ"*ÿ+!%œ, 4096, 0, , 0, V\rGq†â!XÊµ"*ÿ+!%œ, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, ü\$~%œÖ*êri+4,=(?S—, 4096, 0, , 0, ü\$~%œÖ*êri+4,=(?S—, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, F'Yn, 4096, 0, , 0, F'Yn, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, yh\$?Q, 4096, 0, , 0, yh\$?Q, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, Ä%@RlþÜÜF+, 4096, 0, , 0, Ä%@RlþÜÜF+, 4096, -510045568, 0 ) Return: 0		2424
Call System API	API Name: BCryptDecrypt Args: ( efda4b20, Q, 4096, 0, , 0, Q, 4096, -510045568, 0 ) Return: 0		2424
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: a0c		2424
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: ( ebb4e750, 0, 0, 0 ) Return: 1		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2424
Call Internet Helper API	API Name: InternetOpenW Args: ( , 0, , , 10000000 ) Return: cc0004		2424
Call System API	API Name: evtchann.SendEvent Args: ( e), imagepath[%CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE ) Return: 1		2424
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: ( ebb4e5f0, 0, 0, 0 ) Return: 1		2424
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: ( ebb4e5c0, 0, 0, 0 ) Return: 1		2424
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[0], ppid[2424 ) Return: 1		2424
Call System API	API Name: evtchann.SendEvent Args: ( e), imagepath[C:\Program ) Return: 1		2424
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[0], ppid[2424 ) Return: 1		2424
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1, 50020000 ) Return: 9003		2424
Call Internet Helper API	API Name: InternetConnectA Args: ( cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -266527040 ) Return: cc0008		2424
Call Internet Helper API	API Name: HttpOpenRequestA Args: ( cc0008, POST, /OneCollector/1.0/, , , -184683816, -2067004672, -266527040 ) Return: cc000c		2424
Call System API	API Name: WinHttpCloseHandle Args: ( eccc95e0 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: ac0		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: b28		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: b28		2424
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: b34		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: b44		2424
Call Network API	API Name: bind Args: ( b44, 0.0.0.0:49166, 16 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 0.0.0.0:49166		
Call System API	API Name: ConnectEx Args: ( b44, self.events.data.microsoft.com:443, 16, 0, 0, 0, f028c948 ) Return: 0		2424
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: bcc		2424
Call Network API	API Name: send Args: ( b44, ..., 1, 191 ) Return: 0		2424
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one		2424
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f02ca7c0 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: df4		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: df4		2424
Call System API	API Name: DnsQueryEx Args: ( cdn.uci.officeapps.live.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( cdn.uci.officeapps.live.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: bc4		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: bc4		2424
Call Network API	API Name: bind Args: ( bc4, 0.0.0.0:49167, 128 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 0.0.0.0:49167		
Call System API	API Name: ConnectEx Args: ( bc4, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, f40392c8 ) Return: 0		2424
Call Network API	API Name: send Args: ( bc4, ..., 1, 188 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f02c8a80 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: e44		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: e44		2424

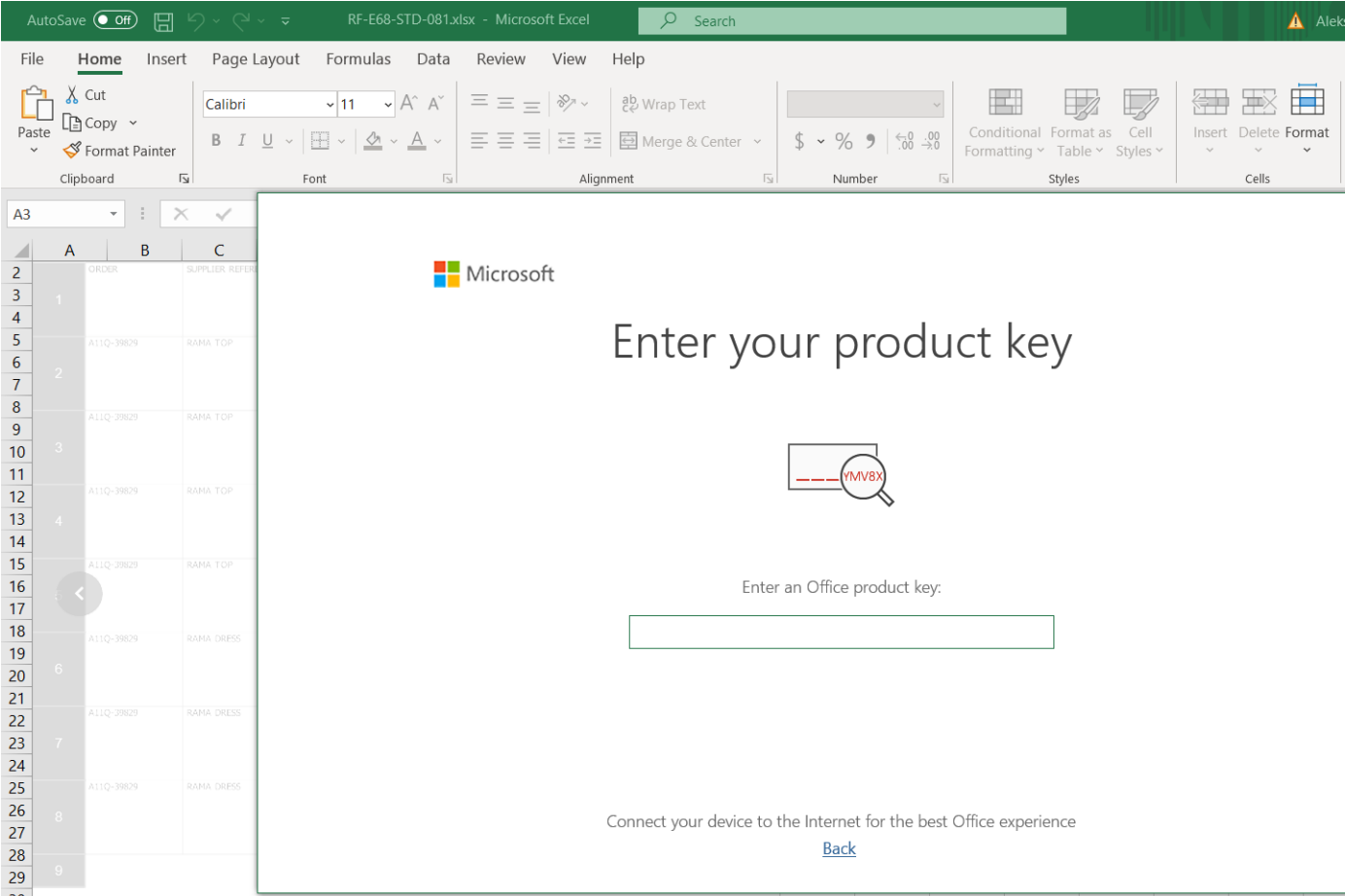
Call System API	API Name: DnsQueryEx Args: ( ctdl.windowsupdate.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( ctdl.windowsupdate.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: df4		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: df4		2424
Call Network API	API Name: bind Args: ( df4, 0.0.0.0:49168, 128 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 0.0.0.0:49168		
Call System API	API Name: ConnectEx Args: ( df4, ctdl.windowsupdate.com:80, 16, 0, 0, 0, f4037748 ) Return: 0		2424
Call Network API	API Name: send Args: ( df4, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?2e65937534f3bed4 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctdl.windowsupdate.com\r\n\r\n, 1, 201 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( eca64a60 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f4036d90 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( e396c980 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( eca64df0 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: bc4		2424
Call Network API	API Name: bind Args: ( bc4, 0.0.0.0:49169, 128 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 0.0.0.0:49169		
Call System API	API Name: ConnectEx Args: ( bc4, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, f40380e8 ) Return: 0		2424
Call Network API	API Name: send Args: ( bc4, ..., 1, 188 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( eca63170 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f4038230 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f40371b0 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: ecc		2424
Call Network API	API Name: bind Args: ( ecc, 127.0.0.1:65200, 128 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 127.0.0.1:65200		
Call System API	API Name: WinHttpCloseHandle Args: ( f02cb3f0 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: f6c		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: f6c		2424
Call System API	API Name: DnsQueryEx Args: ( cdn.uci.officeapps.live.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( cdn.uci.officeapps.live.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: f80		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: f80		2424
Call Network API	API Name: bind Args: ( f80, 0.0.0.0:49170, 128 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 0.0.0.0:49170		
Call System API	API Name: ConnectEx Args: ( f80, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, f40378a8 ) Return: 0		2424
Call Network API	API Name: send Args: ( f80, ..., 1, 188 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( eca63170 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: f74		2424
Call Network API	API Name: bind Args: ( f74, 0.0.0.0:49171, 128 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 0.0.0.0:49171		
Call System API	API Name: ConnectEx Args: ( f74, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, f4038d48 ) Return: 0		2424
Call Network API	API Name: send Args: ( f74, ..., 1, 188 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( eca63170 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: f74		2424
Call Network API	API Name: bind Args: ( f74, 0.0.0.0:49172, 128 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 0.0.0.0:49172		
Call System API	API Name: ConnectEx Args: ( f74, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, f4035908 ) Return: 0		2424
Call Network API	API Name: send Args: ( f74, ..., 1, 188 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( eca64a60 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f4038230 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f4038a70 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 754		2424
Call Network API	API Name: bind Args: ( 754, 0.0.0.0:49173, 128 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 0.0.0.0:49173		
Call System API	API Name: ConnectEx Args: ( 754, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, f4035d28 ) Return: 0		2424
Call Network API	API Name: send Args: ( 754, ..., 1, 188 ) Return: 0		2424
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\1.7\hostproperties.json Type: VSDT_ASCII		2424
Call System API	API Name: WinHttpCloseHandle Args: ( eca63170 ) Return: 1		2424
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\1.7\hostproperties.json Type: VSDT_ASCII		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f4038390 ) Return: 1		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CB956\1CB956 Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CB956 Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\w-& Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2424

Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CE8A3\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CE8A3\1CE8A3 Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2424\0 Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2424\0 Value: None		2424
Call Network API	API Name: socket Args: ( 2, 1, 0 ) Return: 1044		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\SessionId Value: None		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f02caa30 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 1080		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 1080		2424
Call System API	API Name: DnsQueryEx Args: ( gmail.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( gmail.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 1080		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 1080		2424
Call Network API	API Name: bind Args: ( 1080, 0.0.0.0:49174, 128 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 0.0.0.0:49174		
Call System API	API Name: ConnectEx Args: ( 1080, gmail.com:443, 16, 0, 0, 0, f46f1098 ) Return: 0		2424
Call Network API	API Name: send Args: ( 1080, ..., 1, 170 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( effaad50 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f46f4780 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 108c		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 108c		2424
Call System API	API Name: DnsQueryEx Args: ( autodiscover.gmail.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( autodiscover.gmail.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 108c		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 108c		2424
Call Network API	API Name: bind Args: ( 108c, 0.0.0.0:49175, 128 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 0.0.0.0:49175		
Call System API	API Name: ConnectEx Args: ( 108c, autodiscover.gmail.com:443, 16, 0, 0, 0, f46f5138 ) Return: 0		2424
Call Network API	API Name: send Args: ( 108c, ..., 1, 183 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( effaad50 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f46f39c0 ) Return: 1		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\File MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\File MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\User MRU\Liveld_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C495056D56BADD0D4\File MRU\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\User MRU\Liveld_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C495056D56BADD0D4\File MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\User MRU\Liveld_FCD11FD83CCD7F1EEB0847F47EB5220F49E0B81EF722CF9C495056D56BADD0D4\File MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Place MRU\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Place MRU\FOLDERID_Desktop Value: %USERPROFILE%\Desktop\		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Place MRU\FOLDERID_Documents Value: %USERPROFILE%\Documents\		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xls\OpenWithProgids\Excel.Sheet.8 Value: None		2424
Call Internet Helper API	API Name: NetShareEnum Args: ( , 503, 1fcc1318, -1, ed69d060, ed69d068, 0 ) Return: 0		2424
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2424 Info: Enums share folder from API result		
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\9106TLGSSSW5AIPSW0Z3.temp Type: VSDT_COM_DOS		2424
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\9106TLGSSSW5AIPSW0Z3.temp Type: VSDT_COM_DOS		2424
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\b8ab7710df80ab2.customDestinations-ms Type: VSDT_COM_DOS		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CE8A3\1CE8A3 Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CE8A3\ Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ImmersiveWorkbookDirtySentinel Value: 7fffffff		2424
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\7B6031CE.jpeg Type: VSDT_JPG		2424
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\7B6031CE.jpeg Type: VSDT_JPG		2424
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\7B6031CE.jpeg Type: VSDT_JPG		2424
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2424 File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\7B6031CE.jpeg Type: VSDT_JPG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\FB84CAC1.png Type: VSDT_PNG		2424
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\FB84CAC1.png Type: VSDT_PNG		2424
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\FB84CAC1.png Type: VSDT_PNG		2424
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2424 File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\FB84CAC1.png Type: VSDT_PNG		
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1, 50020000 ) Return: 9003		2424
Call Internet Helper API	API Name: InternetConnectA Args: ( cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -198773584 ) Return: cc0008		2424
Call Internet Helper API	API Name: HttpOpenRequestA Args: ( cc0008, POST, /OneCollector/1.0/, , , -184683816, -2067004672, -198773584 ) Return: cc000c		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2424\0 Value: None		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f47dfb00 ) Return: 1		2424



Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: e58		2424
Call Network API	API Name: bind Args: ( e58, 0.0.0.0:49176, 16 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 0.0.0.0:49176		
Call System API	API Name: ConnectEx Args: ( e58, self.events.data.microsoft.com:443, 16, 0, 0, 0, f02968f8 ) Return: 0		2424
Call Network API	API Name: send Args: ( e58, ..., 1, 191 ) Return: 0		2424
Call Filesystem API	API Name: RemoveDirectoryW Args: ( %TEMP%\{996427E9-0900-4C87-9E50-C5EAFE25830}\ ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f47dca40 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 714		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 714		2424
Call System API	API Name: DnsQueryEx Args: ( ctdl.windowsupdate.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( ctdl.windowsupdate.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 1060		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 720		2424
Call Network API	API Name: bind Args: ( 720, 0.0.0.0:49177, 128 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call System API	API Name: ConnectEx Args: ( 720, ctdl.windowsupdate.com:80, 16, 0, 0, 0, f4035fe8 ) Return: 0		2424
Call Network API	API Name: send Args: ( 720, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?4451a85ee3fd6755 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctdl.windowsupdate.com\r\n\r\n, 1, 201 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f42a6d50 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f4037470 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( f47ec120 ) Return: 1		2424
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\1AE205C0.emf ) Return: 1		2424
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1, 50020000 ) Return: 9003		2424
Call Internet Helper API	API Name: InternetConnectA Args: ( cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -323303840 ) Return: cc0008		2424
Call Internet Helper API	API Name: HttpOpenRequestA Args: ( cc0008, POST, /OneCollector/1.0/, , , -184683816, -2067004672, -323303840 ) Return: cc000c		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: df4		2424
Call Network API	API Name: bind Args: ( df4, 0.0.0.0:49178, 16 ) Return: 0		2424
Detection	Threat Characteristic: Listens on port 0.0.0.0:49178		
Call System API	API Name: ConnectEx Args: ( df4, self.events.data.microsoft.com:443, 16, 0, 0, 0, f02922f8 ) Return: 0		2424
Call Network API	API Name: send Args: ( df4, ..., 1, 191 ) Return: 0		2424

▼ Screenshot



▼ Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	1B87A12587E64C861DD1BC2393D98A295FDC5475
SHA-256	9DEFBF30CBA0EA1800B56F533A219E843238D1AA679299039D3396CAAAA6C56D
MD5	7CF448383FBD330DCCBB937198018AAB
Size	2333254 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

▼ Network Destinations

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

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

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
excel.exe.db-wal	No risk	-	-	-	4152	8BE2B270E80D92D47C772C20478D695B0E360B98
excel.exe.db-shm	No risk	-	-	-	32768	071EDF7E52C0C78527861C7572C9650EF504906F
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	302	C2B2CDC61F79169B400CAF1C336DFA1B161E94F4
{0B097597-79B2-479D-B1C9-2FB8B879B363} - OProcSessId.dat	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
App_1616237086612139400_0B097597-79B2-479D-B1C9-2FB8B879B363.log	No risk	-	-	-	20971520	7BBA7881AD9C06D876838820B006DA463BAAD7D6
App_1616237086617297800_0B097597-79B2-479D-B1C9-2FB8B879B363.log	No risk	-	-	-	20971520	9674344C90C2F0646F0B78026E127C9B86E3AD77
F92EC12F.emf	No risk	-	-	-	653280	56AA3848A35179465E6C05D9D3C3F3DD8B651BEA
hostproperties.json	No risk	-	-	-	185	BC583C6DD14A35DA17CF1197B25D3A0E4B4D83BF
C8ABD215.jpeg	No risk	-	-	-	45677	4545D7788B69E441BDCD8B2A667ED5B59985E12B

▼ Analysis

Event Type	Details	Parent PID	PID
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ClientTelemetry\Sampling\1 Value: None		2756
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2756\ Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2756\ Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2756
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2756
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\>n? Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ImmersiveWorkbookDirtySentinel Value: 0		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\ExcelWorkbookOpenedCount Value: 0		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\EXCEL\2704\ Value: None		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\EXCEL\2704\ Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2756\ Value: None		2756
Call Filesystem API	API Name: DeleteFileW Args: ( %TEMP%\Diagnostics\EXCEL\App_1600985250979406400_37DFED58-65EC-4733-9903-AF526D736AF9.log ) Return: 1		2756
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: ( ROOT\CIMV2, en-US,en, 0, 0, 286f470 ) Return: 0		2756
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 286f470 ) Return: 0		2756
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 286f3b0 ) Return: 0		2756
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: ( UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0 ) Return: 0		2756
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE "%PHYSICALDRIVE0%", 30, 0, 286f3b0 ) Return: 0		2756
Call WMI API	API Name: Win32_DiskDrive::Get Args: ( SerialNumber, 0, GJZ3J0NSM, 0, 0 ) Return: 0		2756
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag=Physical Memory 0', 30, 0, 286f3b0 ) Return: 0		2756
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\{f52c64b7e\LanguageList Value: en-US\0en\0		2756

Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: ( ROOT\CIMV2, en-US,en, 0, 0, 1e5e2a0 ) Return: 0		2756
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, 1e5e2a0 ) Return: 0		2756
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, 1e5e1e0 ) Return: 0		2756
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: ( UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0 ) Return: 0		2756
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE "%PHYSICALDRIVE0%", 30, 0, 1e5e1e0 ) Return: 0		2756
Call WMI API	API Name: Win32_DiskDrive::Get Args: ( SerialNumber, 0, GJZ3J0NSM, 0, 0 ) Return: 0		2756
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag="Physical Memory 0", 30, 0, 1e5e1e0 ) Return: 0		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastSyncTimeExcel Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastWriteTimeExcel Value: None		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems>n? Value: None		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2756
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2756
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\0~? Value: None		2756
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2756
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CF611\ Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CF611\1CF611 Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CF611\1CF611 Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CF611\1CF611 Value: None		2756
Call System API	API Name: evtchann.SendEvent Args: ( e, imagePath[%CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE ) Return: 1		2756
Call System API	API Name: evtchann.SendEvent Args: ( e, pid[0], ppid[2756 ] Return: 1		2756
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: ( 265e0f0, 0, 0, 0 ) Return: 1		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2756
Call Internet Helper API	API Name: InternetOpenW Args: ( , 0 , , 10000000 ) Return: cc0004		2756
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: ( 265df90, 0, 0, 0 ) Return: 1		2756
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: ( 265df60, 0, 0, 0 ) Return: 1		2756
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: a30		2756
Call System API	API Name: evtchann.SendEvent Args: ( e, imagePath[C:\Program ) Return: 1		2756
Call System API	API Name: evtchann.SendEvent Args: ( e, pid[0], ppid[2756 ] Return: 1		2756
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1, 50020000 ) Return: 9003		2756
Call Internet Helper API	API Name: InternetConnectA Args: ( cc0004, self.events.data.microsoft.com, 443, , , 3, 0, 104298928 ) Return: cc0008		2756
Call Internet Helper API	API Name: HttpOpenRequestA Args: ( cc0008, POST, /OneCollector/1.0/, , , 117830344, -2067004672, 104298928 ) Return: cc000c		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 6799890 ) Return: 1		2756
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: af0		2756
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: af0		2756
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1, 40006000 ) Return: 87		2756
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1c, 40026000 ) Return: 9003		2756
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: afc		2756
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: afc		2756
Call Network API	API Name: bind Args: ( afc, 0.0.0.0:49168, 16 ) Return: 0		2756
Call System API	API Name: ConnectEx Args: ( afc, self.events.data.microsoft.com:443, 16, 0, 0, 0, 63b71d8 ) Return: 0		2756
Call Network API	API Name: send Args: ( afc, ..., 1, 191 ) Return: 0		2756
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one		2756
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Val ue: None		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2a57f30 ) Return: 1		2756
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: d6c		2756
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: dc8		2756
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: dc8		2756
Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 87		2756
Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 9003		2756
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: d5c		2756
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: d5c		2756
Call Network API	API Name: bind Args: ( d5c, 0.0.0.0:49169, 128 ) Return: 0		2756
Call System API	API Name: ConnectEx Args: ( d5c, ctldl.windowsupdate.com:80, 16, 0, 0, 0, 62f5cf8 ) Return: 0		2756
Call Network API	API Name: send Args: ( d5c, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?4a54d02e98e80c7a 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		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2a68c60 ) Return: 1		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 62f93e0 ) Return: 1		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 6364870 ) Return: 1		2756
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 628		2756
Call Network API	API Name: bind Args: ( 628, 127.0.0.1:55275, 128 ) Return: 0		2756
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\1.7\hostproperties.json Type: VSDT_ASCII		2756

Write File	Path: %LOCALAPPDATA%\Microsoft\Office\16.0\Wef\CustomFunctions\sv1.7\hostproperties.json Type: VSDT_ASCII		2756
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: f80		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CF611\1CF611 Value: None		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1CF611\ Value: None		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\0~? Value: None		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\StartupItems\ Value: None		2756
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2756
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\ Value: None		2756
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\ Value: None		2756
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D201E\ Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DocumentRecovery\1D201E\1D201E Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2756\0 Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\EXCEL\2756\0 Value: None		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2a588f0 ) Return: 1		2756
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: fcc		2756
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: fcc		2756
Call System API	API Name: DnsQueryEx Args: ( cdn.uci.officeapps.live.com, 1, 40006000 ) Return: 87		2756
Call System API	API Name: DnsQueryEx Args: ( cdn.uci.officeapps.live.com, 1c, 40026000 ) Return: 9003		2756
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: fcc		2756
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: fcc		2756
Call Network API	API Name: bind Args: ( fcc, 0.0.0.0:49170, 128 ) Return: 0		2756
Call System API	API Name: ConnectEx Args: ( fcc, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 2ce8d88 ) Return: 0		2756
Call Network API	API Name: send Args: ( fcc, ..., 1, 188 ) Return: 0		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2bca490 ) Return: 1		2756
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: fcc		2756
Call Network API	API Name: bind Args: ( fcc, 0.0.0.0:49171, 128 ) Return: 0		2756
Call System API	API Name: ConnectEx Args: ( fcc, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 2ceae88 ) Return: 0		2756
Call Network API	API Name: send Args: ( fcc, ..., 1, 188 ) Return: 0		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2bc7d60 ) Return: 1		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2ce8d70 ) Return: 1		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2cea210 ) Return: 1		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2a57f30 ) Return: 1		2756
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: fe0		2756
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: fe0		2756
Call System API	API Name: DnsQueryEx Args: ( cdn.uci.officeapps.live.com, 1, 40006000 ) Return: 87		2756
Call System API	API Name: DnsQueryEx Args: ( cdn.uci.officeapps.live.com, 1c, 40026000 ) Return: 9003		2756
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: ff8		2756
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: ff8		2756
Call Network API	API Name: bind Args: ( ff8, 0.0.0.0:49172, 128 ) Return: 0		2756
Call System API	API Name: ConnectEx Args: ( ff8, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 2ce8c28 ) Return: 0		2756
Call Network API	API Name: send Args: ( ff8, ..., 1, 188 ) Return: 0		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2bc8480 ) Return: 1		2756
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: ff8		2756
Call Network API	API Name: bind Args: ( ff8, 0.0.0.0:49173, 128 ) Return: 0		2756
Call System API	API Name: ConnectEx Args: ( ff8, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 2ce9ca8 ) Return: 0		2756
Call Network API	API Name: send Args: ( ff8, ..., 1, 188 ) Return: 0		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2bc7d60 ) Return: 1		2756
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: ff8		2756
Call Network API	API Name: bind Args: ( ff8, 0.0.0.0:49174, 128 ) Return: 0		2756
Call System API	API Name: ConnectEx Args: ( ff8, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 2ce7d08 ) Return: 0		2756
Call Network API	API Name: send Args: ( ff8, ..., 1, 188 ) Return: 0		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2bca490 ) Return: 1		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2ce8ab0 ) Return: 1		2756
Call System API			
Call System API	API Name: WinHttpCloseHandle Args: ( 2ce9710 ) Return: 1		2756
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: fcc		2756
Call Network API	API Name: bind Args: ( fcc, 0.0.0.0:49175, 128 ) Return: 0		2756
Call System API	API Name: ConnectEx Args: ( fcc, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, 2ce9468 ) Return: 0		2756
Call Network API	API Name: send Args: ( fcc, ..., 1, 188 ) Return: 0		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2bc7d60 ) Return: 1		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2ce7a30 ) Return: 1		2756
Call Network API	API Name: socket Args: ( 2, 1, 0 ) Return: ff0		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\SessionId Value: None		2756
Call System API	API Name: WinHttpCloseHandle Args: ( a92fce0 ) Return: 1		2756
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 1020		2756
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 1020		2756
Call System API	API Name: DnsQueryEx Args: ( gmail.com, 1, 40006000 ) Return: 87		2756
Call System API	API Name: DnsQueryEx Args: ( gmail.com, 1c, 40026000 ) Return: 9003		2756
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 1020		2756
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 1020		2756
Call Network API	API Name: bind Args: ( 1020, 0.0.0.0:49176, 128 ) Return: 0		2756

Call System API	API Name: ConnectEx Args: ( 1020, gmail.com:443, 16, 0, 0, 0, 2c9b548 ) Return: 0		2756
Call Network API	API Name: send Args: ( 1020, ..., 1, 170 ) Return: 0		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2bc99e0 ) Return: 1		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2c9e970 ) Return: 1		2756
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: 1028		2756
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 1028		2756
Call System API	API Name: DnsQueryEx Args: ( autodiscover.gmail.com, 1, 40006000 ) Return: 87		2756
Call System API	API Name: DnsQueryEx Args: ( autodiscover.gmail.com, 1c, 40026000 ) Return: 9003		2756
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 1028		2756
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 1028		2756
Call Network API	API Name: bind Args: ( 1028, 0.0.0.0:49177, 128 ) Return: 0		2756
Call System API	API Name: ConnectEx Args: ( 1028, autodiscover.gmail.com:443, 16, 0, 0, 0, 2c9c728 ) Return: 0		2756
Call Network API	API Name: send Args: ( 1028, ..., 1, 183 ) Return: 0		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2bc8ba0 ) Return: 1		2756
Call System API	API Name: WinHttpCloseHandle Args: ( 2c9d8f0 ) Return: 1		2756
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security\Trusted Documents\ Value: None		2756
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 19b07c5		2756

▼ Screenshot

↶

Activate Windows

🔍

Activate Windows

This version of Windows is expired. Install the latest version to activate.

Install the latest version of Windows

▼ 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	738E9370EF36110EA752304C9BBC67EFE043ED47
SHA-256	E302FC5D511C8C1EFE0C45FE73F994F6896F19627BB013CA489919D113B6BD9C
MD5	8F19AC5BC33213CE27E70B42C3651A58
Size	127575 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
ctdl.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/officeaugmenta tion/searchendpoint/	Computers / Internet	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm
https://self.events.data.microsoft.com/OneCollect or/1.0/	Business / Economy Computers / Internet Cloud Applications	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
winword.exe.db-shm	No risk	-	-	-	32768	DC6335783E40DE4A450294E1678120EC642BEEEF
~\RS\{943B663E-EEFA-4194-935F-67562721809A}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
~\$crosoft_Office_Word_Macro-En abled_Document1.docm.docx	No risk	-	-	-	162	5703FB8F6957EAA20D0023BD76B9A1C723A3BA8B
~\$Normal.dotm	No risk	-	-	-	162	B668AA9583C3EDA7FF3C29D2C013261E88311E1D
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	302	54CD0F99A3CA8C78ECF4F5F485072EA71BA6B24E
Word.SurveyHistoryStats.json	No risk	-	-	-	14	2FD90B4EC32804DFF7A41B6E63C8B0A40B592113
Word.GovernedChannelStates.js on	No risk	-	-	-	416	E4BB75AD0271B53C30388C18356CDEA1BADF346C
Word.Settings.json	No risk	-	-	-	87	5281EAE96EFDE7B0E16A1D977F005F0D3BD7AAD0
App_1616237349006017900_2748C16A-3AA6-4EAC-9D15-652278EFE518.log	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
winword.exe.db-wal	No risk	-	-	-	428512	983C409C91BE97B1F790F1E49C42E926BABE8FDE

▼ Analysis

Event Type	Details	Parent PID	PID
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ClientTelemetry\Sampling\0 Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2424\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2424\0 Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\ Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\y<8 Value: None		2424
Call Filesystem API	API Name: DeleteFileW Args: ( %TEMP%\Diagnostics\WINWORD\App_1600985251099791600_A16BA699-DE8A-473F-B54F-C8D59B3C1D07.log ) Return: 1		2424
Delete File	Path: %TEMP%\Diagnostics\WINWORD\App_1600985251099791600_A16BA699-DE8A-473F-B54F-C8D59B3C1D07.log Type: VSDT_EMPTY		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2532\0 Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2532\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2424\0 Value: None		2424
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		2424
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		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5807}\ Value: None		2424
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		2424
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		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2424
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		2424

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		2424
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		2424
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		2424
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		2424
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		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ULSAI\Categories Value: 6, 10		2424
Call WMI API	API Name: IWbemLevel1Login::NTLMLLogin Args: ( ROOT\CIMV2, en-US,en, 0, 0, ac0bf180 ) Return: 0		2424
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, ac0bf180 ) Return: 0		2424
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, ac0bf0c0 ) Return: 0		2424
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: ( UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0 ) Return: 0		2424
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE "%PHYSICALDRIVE0%", 30, 0, ac0bf0c0 ) Return: 0		2424
Call WMI API	API Name: Win32_DiskDrive::Get Args: ( SerialNumber, 0, GJZ3J0NSM, 0, 0 ) Return: 0		2424
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag=Physical Memory 0', 30, 0, ac0bf0c0 ) Return: 0		2424
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\{f52c64b7e\LanguageList Value: en-US\0en\0		2424
Call WMI API	API Name: IWbemLevel1Login::NTLMLLogin Args: ( ROOT\CIMV2, en-US,en, 0, 0, ac0bdd0 ) Return: 0		2424
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, ac0bdd0 ) Return: 0		2424
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, ac0bde10 ) Return: 0		2424
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: ( UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0 ) Return: 0		2424
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE "%PHYSICALDRIVE0%", 30, 0, ac0bde10 ) Return: 0		2424
Call WMI API	API Name: Win32_DiskDrive::Get Args: ( SerialNumber, 0, GJZ3J0NSM, 0, 0 ) Return: 0		2424
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag=Physical Memory 0', 30, 0, ac0bde10 ) Return: 0		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\=( & Value: None		2424
Add File	Path: %APPDATA%\Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS		2424
Write File	Path: %APPDATA%\Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\=( & Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastSyncTimeWord Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastWriteTimeWord Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2424\0 Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\8, & Value: None		2424
Call Filesystem API	API Name: DeleteFileW Args: ( %WorkingDir%\~\$crossoft_Office_Word_Macro-Enabled_Document1.docm.docx ) Return: 1		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\8, & Value: None		2424
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml ) Return: 0		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\y<& Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\ Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2424\0 Value: None		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: a2c		2424
Call Network API	API Name: bind Args: ( a2c, 127.0.0.1:65200, 128 ) Return: 0		2424
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: adc		2424
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: ( abebe160, 0, 0, 0 ) Return: 1		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Proxy\Enable Value: 0		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Proxy\Server Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Proxy\Override Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2424
Call Internet Helper API	API Name: InternetOpenW Args: ( , 0, , , 10000000 ) Return: cc0004		2424
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: ( abebe000, 0, 0, 0 ) Return: 1		2424
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: ( abebdfd0, 0, 0, 0 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 1, 0 ) Return: a88		2424
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: b68		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\SessionId Value: None		2424
Call System API	API Name: WinHttpCloseHandle Args: ( adaec0a0 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: bc0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( adaec0a0 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: c30		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: c30		2424
Call System API	API Name: DnsQueryEx Args: ( gmail.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( gmail.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: c30		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: c30		2424
Call Network API	API Name: bind Args: ( c30, 0.0.0.0:49166, 128 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( c30, gmail.com:443, 16, 0, 0, 0, b4480438 ) Return: 0		2424

Call Network API	API Name: send Args: ( c30, ..., 1, 170 ) Return: 0		2424
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		2424
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4327cc0 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b447e5e0 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: c30		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: c30		2424
Call System API	API Name: DnsQueryEx Args: ( autodiscover.gmail.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( autodiscover.gmail.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: c3c		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: c3c		2424
Call Network API	API Name: bind Args: ( c3c, 0.0.0.0:49167, 128 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( c3c, autodiscover.gmail.com:443, 16, 0, 0, 0, b44814b8 ) Return: 0		2424
Call Network API	API Name: send Args: ( c3c, ..., 1, 183 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b410abe0 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4481340 ) Return: 1		2424
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1, 50020000 ) Return: 9003		2424
Call Internet Helper API	API Name: InternetConnectA Args: ( cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -1379341280 ) Return: cc0008		2424
Call Internet Helper API	API Name: HttpOpenRequestA Args: ( cc0008, POST, /OneCollector/1.0/, , , -1221005320, -2067004672, -1379341280 ) Return: cc000c		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: e68		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: e68		2424
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: e6c		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: e6c		2424
Call Network API	API Name: bind Args: ( e6c, 0.0.0.0:49168, 16 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( e6c, self.events.data.microsoft.com:443, 16, 0, 0, 0, b4348098 ) Return: 0		2424
Call Network API	API Name: send Args: ( e6c, ..., 1, 191 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4103b40 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: ee0		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: ee0		2424
Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: e64		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: e64		2424
Call Network API	API Name: bind Args: ( e64, 0.0.0.0:49169, 128 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( e64, ctldl.windowsupdate.com:80, 16, 0, 0, 0, b447fa98 ) Return: 0		2424
Call Network API	API Name: send Args: ( e64, GET /msdownload/update/v3/static/trustedr/en/disallowedcerts/cab?772aca017183cad4d 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		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4108120 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4481340 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4715ce0 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: ed4		2424
Call Internet Helper API	API Name: InternetOpenW Args: ( , 0, , , 10000000 ) Return: cc0008		2424
Call System API	API Name: DnsQueryEx Args: ( augmentation.osi.office.net, 1, 50020000 ) Return: 9003		2424
Call Internet Helper API	API Name: InternetConnectW Args: ( cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0 ) Return: cc000c		2424
Call Internet Helper API	API Name: HttpOpenRequestW Args: ( cc000c, GET, /officeaugmentation/searchendpoint/, , , 0, -2134884352, -1309066592 ) Return: cc0010		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: f30		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: f30		2424
Call System API	API Name: DnsQueryEx Args: ( augmentation.osi.office.net, 1, 40006000 ) Return: 87		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b41070e0 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: f18		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: f18		2424
Call System API	API Name: DnsQueryEx Args: ( cdn.uci.officeapps.live.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( cdn.uci.officeapps.live.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: f18		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: f18		2424
Call Network API	API Name: bind Args: ( f18, 0.0.0.0:49170, 128 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( f18, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, b447e5f8 ) Return: 0		2424
Call Network API	API Name: send Args: ( f18, ..., 1, 188 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4109da0 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: f18		2424
Call Network API	API Name: bind Args: ( f18, 0.0.0.0:49171, 128 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( f18, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, b4480598 ) Return: 0		2424
Call Network API	API Name: send Args: ( f18, ..., 1, 188 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4108f60 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b447ee20 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b447fea0 ) Return: 1		2424
Call System API	API Name: DnsQueryEx Args: ( augmentation.osi.office.net, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: f18		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: f38		2424

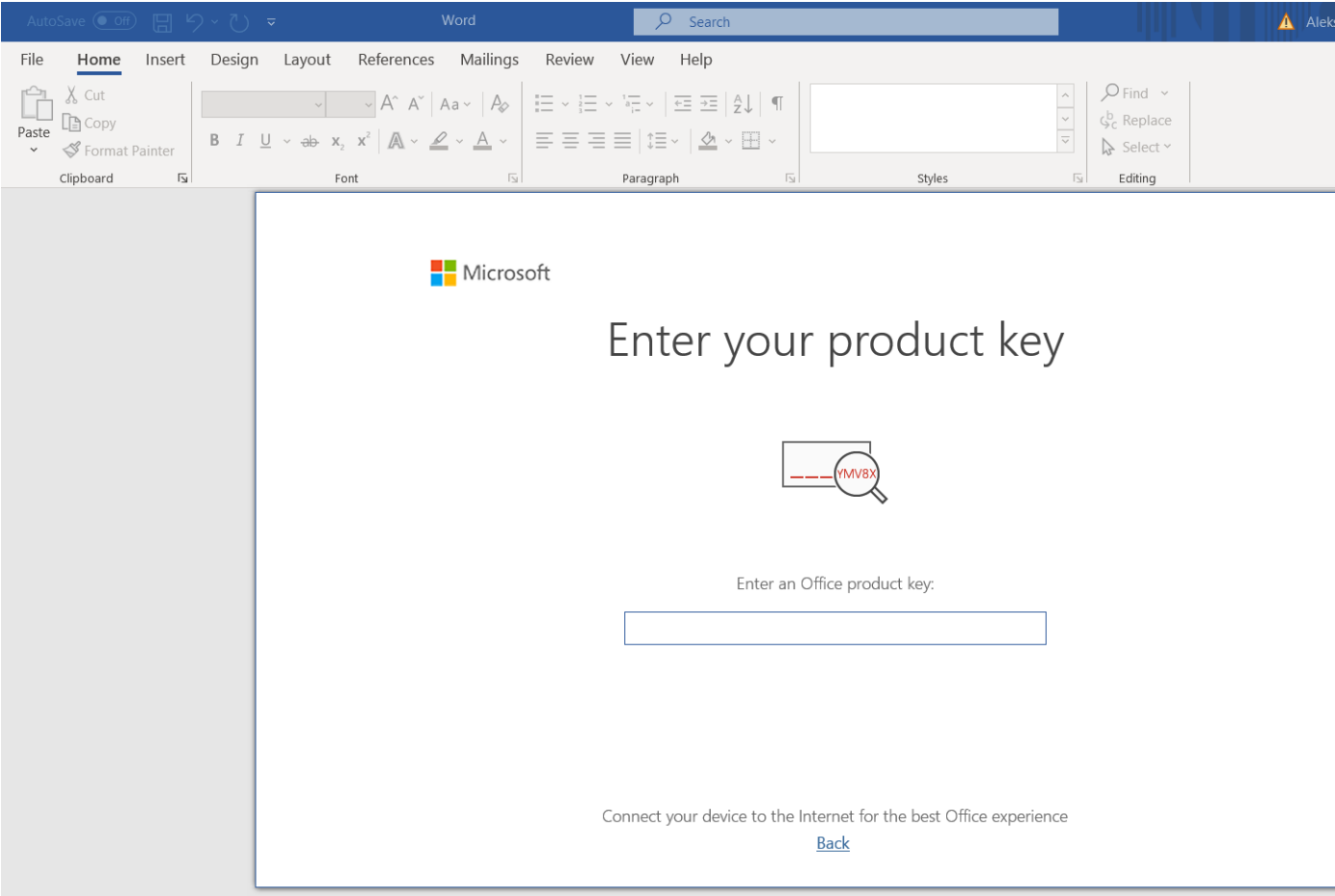


Call Network API	API Name: bind Args: ( f38, 0.0.0.0:49172, 16 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( f38, augmentation.osi.office.net:443, 16, 0, 0, 0, ae1ff9d8 ) Return: 0		2424
Call Network API	API Name: send Args: ( f38, ..., 1, 188 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4106e70 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: ed4		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: ed4		2424
Call System API	API Name: DnsQueryEx Args: ( cdn.uci.officeapps.live.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( cdn.uci.officeapps.live.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: f24		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: f24		2424
Call Network API	API Name: bind Args: ( f24, 0.0.0.0:49173, 128 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( f24, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, b447e498 ) Return: 0		2424
Call Network API	API Name: send Args: ( f24, ..., 1, 188 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b410af70 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: f24		2424
Call Network API	API Name: bind Args: ( f24, 0.0.0.0:49174, 128 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( f24, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, b447ee38 ) Return: 0		2424
Call Network API	API Name: send Args: ( f24, ..., 1, 188 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4109a10 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: f24		2424
Call Network API	API Name: bind Args: ( f24, 0.0.0.0:49175, 128 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( f24, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, b447f3b8 ) Return: 0		2424
Call Network API	API Name: send Args: ( f24, ..., 1, 188 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b410af70 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b447e740 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b447fea0 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: f24		2424
Call Network API	API Name: bind Args: ( f24, 0.0.0.0:49176, 128 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( f24, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, b4480598 ) Return: 0		2424
Call Network API	API Name: send Args: ( f24, ..., 1, 188 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b410abe0 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b447e5e0 ) Return: 1		2424
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1, 50020000 ) Return: 9003		2424
Call Internet Helper API	API Name: InternetConnectA Args: ( cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -1379354528 ) Return: cc0008		2424
Call Internet Helper API	API Name: HttpOpenRequestA Args: ( cc0008, POST, /OneCollector/1.0/, , , -1221005320, -2067004672, -1379354528 ) Return: cc000c		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: efc		2424
Call Network API	API Name: bind Args: ( efc, 0.0.0.0:49177, 16 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( efc, self.events.data.microsoft.com:443, 16, 0, 0, 0, ae1f16c8 ) Return: 0		2424
Call Network API	API Name: send Args: ( efc, ..., 1, 191 ) Return: 0		2424
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1, 50020000 ) Return: 9003		2424
Call Internet Helper API	API Name: InternetConnectA Args: ( cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -1379340176 ) Return: cc0008		2424
Call Internet Helper API	API Name: HttpOpenRequestA Args: ( cc0008, POST, /OneCollector/1.0/, , , -1221005320, -2067004672, -1379340176 ) Return: cc000c		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 78c		2424
Call Network API	API Name: bind Args: ( 78c, 0.0.0.0:49178, 16 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( 78c, self.events.data.microsoft.com:443, 16, 0, 0, 0, ae1f2fb8 ) Return: 0		2424
Call Network API	API Name: send Args: ( 78c, ..., 1, 191 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4103b40 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: f2c		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: f2c		2424
Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 87		2424
Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: ed4		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: ed4		2424
Call Network API	API Name: bind Args: ( ed4, 0.0.0.0:49179, 128 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( ed4, ctldl.windowsupdate.com:80, 16, 0, 0, 0, b4480b18 ) Return: 0		2424
Call Network API	API Name: send Args: ( ed4, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?86984e92a0192ce3 HTTP/1.1\r\nConnection: Keep-Alive\r\nnAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4107a00 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4480420 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4716880 ) Return: 1		2424
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1, 50020000 ) Return: 9003		2424
Call Internet Helper API	API Name: InternetConnectA Args: ( cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -1379341280 ) Return: cc0008		2424
Call Internet Helper API	API Name: HttpOpenRequestA Args: ( cc0008, POST, /OneCollector/1.0/, , , -1221005320, -2067004672, -1379341280 ) Return: cc000c		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4106e70 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: a28		2424
Call Network API	API Name: bind Args: ( a28, 0.0.0.0:49180, 16 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( a28, self.events.data.microsoft.com:443, 16, 0, 0, 0, b43e0098 ) Return: 0		2424
Call Network API	API Name: send Args: ( a28, ..., 1, 191 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4107350 ) Return: 1		2424
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: f44		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: f44		2424
Call System API	API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 87		2424














Call System API	API Name: DnsQueryEx Args: ( ctdl.windowsupdate.com, 1c, 40026000 ) Return: 9003		2424
Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 78c		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 78c		2424
Call Network API	API Name: bind Args: ( 78c, 0.0.0.0:49181, 128 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( 78c, ctdl.windowsupdate.com:80, 16, 0, 0, 0, b4480178 ) Return: 0		2424
Call Network API	API Name: send Args: ( 78c, GET /msdownload/update/v3/static/trusted/en/disaallowedcertsl.cab?8e68452719bb15dc HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctdl.windowsupdate.com\r\n\r\n, 1, 201 ) Return: 0		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b410abe0 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b4481a20 ) Return: 1		2424
Call System API	API Name: WinHttpCloseHandle Args: ( b47162b0 ) Return: 1		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\WordName Value: Word (Unlicensed Product)		2424
Call System API	API Name: CryptGenKey Args: ( a4a34360, 6610, 1, ac0bed48 ) Return: 1		2424
Call System API	API Name: CryptExportKey Args: ( b43e0c60, b43e0480, 1, 0, 0, ac0bed40 ) Return: 1		2424
Call System API	API Name: CryptExportKey Args: ( b43e0c60, b43e0480, 1, 0, b4724810, ac0bed40 ) Return: 1		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Toolbars\Settings\Microsoft Word Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Data\Settings Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Options\AppWindowPos Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2424\0 Value: None		2424
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Templates~\$Normal.dotm ) Return: 1		2424
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content Word~-WRS\943B663E-EEFA-4194-935F-67562721809A).tmp ) Return: 1		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2424\0 Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2424\0 Value: None		2424
Delete File	Path: %APPDATA%\Microsoft\Templates~\$Normal.dotm Type: VSDT_COM_DOS		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2424\0 Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2424\0 Value: None		2424
Call Filesystem API	API Name: RemoveDirectoryW Args: ( %TEMP%\{CACE9D50-028D-4313-B404-CD5D2BCFABDC}\ ) Return: 1		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93A0-2BC6273BC8E4}\ Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\F562BB8E-422D-4B5C-B20E-90D710F7D11C\ Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\ Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ULSMonitor\ Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\ Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\DAF0B914-9C1C-450A-81B2-FAE7244F6FFA\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\DAF0B914-9C1C-450A-81B2-FAE7244F6FFA\5 Value: 0		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\DAF0B914-9C1C-450A-81B2-FAE7244F6FFA\Categories Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\A1B69D49-2195-4F59-9D33-BDF30C0FE473\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\A1B69D49-2195-4F59-9D33-BDF30C0FE473\4 Value: 0		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\A1B69D49-2195-4F59-9D33-BDF30C0FE473\Categories Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07\5 Value: 0		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07\Categories Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\F562BB8E-422D-4B5C-B20E-90D710F7D11C\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\F562BB8E-422D-4B5C-B20E-90D710F7D11C\4 Value: 0		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\F562BB8E-422D-4B5C-B20E-90D710F7D11C\Categories Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\02FD33DF-F746-4A10-93A0-2BC6273BC8E4\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\02FD33DF-F746-4A10-93A0-2BC6273BC8E4\4 Value: 0		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\02FD33DF-F746-4A10-93A0-2BC6273BC8E4\Categories Value: None		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ULSMonitor\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ULSMonitor\ULSAI\Categories Value: 6, 10		2424
Add File	Path: %TEMP%\Diagnostics\WINWORD\App_1616237349004733500_2748C16A-3AA6-4EAC-9D15-652278EFE518.log Type: VSDT_ASCII		2424
Write File	Path: %TEMP%\Diagnostics\WINWORD\App_1616237349004733500_2748C16A-3AA6-4EAC-9D15-652278EFE518.log Type: VSDT_ASCII		2424
Add File	Path: %TEMP%\Diagnostics\WINWORD\App_1616237349006017900_2748C16A-3AA6-4EAC-9D15-652278EFE518.log Type: VSDT_EMPTY		2424
Write File	Path: %TEMP%\Diagnostics\WINWORD\App_1616237349006017900_2748C16A-3AA6-4EAC-9D15-652278EFE518.log Type: VSDT_EMPTY		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Licensing\BootTimeSkuOverride\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Licensing\BootTimeSkuOverride\DC5CCACD-A7AC-4FD3-9F70-9454B5DE5161\ Value: {D7279DD0-E175-49FE-A623-8FC2FC00AFC4}		2424
Call System API	API Name: DnsQueryEx Args: ( self.events.data.microsoft.com, 1, 50020000 ) Return: 9003		2424

Call Internet Helper API	API Name: InternetConnectA Args: ( cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -1379352320 ) Return: cc0008		2424
Call Internet Helper API	API Name: HttpOpenRequestA Args: ( cc0008, POST, /OneCollector/1.0/, , , -1221005320, -2067004672, -1379352320 ) Return: cc000c		2424
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 378		2424
Call Network API	API Name: bind Args: ( 378, 0.0.0.0:49182, 16 ) Return: 0		2424
Call System API	API Name: ConnectEx Args: ( 378, self.events.data.microsoft.com:443, 16, 0, 0, 0, b43d64d8 ) Return: 0		2424
Call Network API	API Name: send Args: ( 378, ..., 1, 191 ) Return: 0		2424
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\winword.exe.db-shm ) Return: 1		2424
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\OTele\winword.exe.db-wal ) Return: 1		2424
Call Filesystem API	API Name: DeleteFileW Args: ( %TEMP%\{2748C16A-3AA6-4EAC-9D15-652278EFE518} - OProcSessId.dat ) Return: 1		2424
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2424\ Value: None		2424
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2424\0 Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2424\0 Value: None		2424
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2424\ Value: None		2424

▼ Screenshot



Process Graph Legend

Node	Notable Threat Characteristics		
 Submitted sample	 Anti-security, self-preservation	 Malformed, defective, or with known malware traits	
 Root process	 Autostart or other system reconfiguration	 Process, service, or memory object change	
 Child process	 Deception, social engineering	 Rootkit, cloaking	
———— Direct event	 File drop, download, sharing, or replication	 Suspicious network or messaging activity	
- - - - - Indirect event	 Hijack, redirection, or data theft		
 Created	Event actions		